

Microsoft®

Microsoft 安全性解決方案

Windows Server 2003 資訊安全手冊



Microsoft®

Windows Server 2003

目錄

1. 簡介 Windows Server 2003 安全性手冊.....	2
2. 設定網域基礎架構.....	14
3. 建立成員伺服器基礎.....	44
4. 補強網域控制站.....	154
5. 補強基礎架構伺服器.....	176
6. 補強檔案伺服器.....	186
7. 補強列印伺服器.....	193
8. 補強 IIS 伺服器.....	201
9. 補強 IAS 伺服器.....	224
10. 補強憑證服務伺服器.....	229
11. 補強防禦主機.....	243
12. 結論.....	262

1. 簡介 Windows Server 2003 安全性手冊

概觀

歡迎閱讀這份 Microsoft Windows Server 2003 安全性手冊！這份手冊的設計，能提供給您最佳的資訊，以便您評估與了解在系統環境中 Microsoft® Windows Server™ 2003 所可能產生的安全性風險。這份手冊中各章節都提供詳細的指引，並將重點放在在 Windows Server 2003 中各種可能的安全性設定組態與功能，使得您能夠處理在環境中所發現的安全性危機。如果您是在 Windows Server 2003 環境中擔任顧問、設計師，或系統工程師，那麼本手冊可說是相當適合您。

這份指引的內容已經過 Microsoft 工程團隊、顧問、支援工程師，以及顧客和合作伙伴的檢閱與認可，因此它是：

- 經證實的 – 以實戰經驗為基礎。
- 具權威性 – 提供可用的最佳意見。
- 具準確性 – 經過技術確認和測試。
- 可執行的 – 提供達到成功的步驟。
- 具相關性 – 提出真實世界的安全性考量。

與在各種不同的環境中導入 Windows Server 2003、Windows® XP 和 Windows® 2000 的顧問及系統工程師一起工作，幫助我們能夠確立最新最佳的實施方針，來保護這些伺服器 and 用戶端的安全。在這手冊中提供已經很詳細地提供這些資訊。

附上的手冊，《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》，提供了對 Windows Server 2003 和 Windows XP 中，所有主要的安全性設定全面性的看法。本手冊的第二章到第十一章，包括了詳細一步一步安全性處理、程序和建議，提供您將組織中執行 Windows Server 2003 的電腦的安全狀態，轉換至更高安全性所需的工作清單。如果您需要更多關於這份文件背後觀念的深入討論，請參考以下資源，例如 Microsoft Windows 2003 Server Resource Kit、Microsoft Windows XP Resource Kit、Microsoft Windows 2000 Security Resource Kit，和 Microsoft TechNet。

執行摘要

不論您的環境如何，我們都強烈地建議您認真看待安全性這問題。許多企業組織犯了一個錯誤，就是低估了他們的資訊技術 (IT) 環境的價值，而這通常是因為他們忽略了重大的間接成本。如果您環境中的伺服器受到的攻擊嚴重程度十分大時，可能整個組織都會受到嚴重傷害。例如，如果您的組織網站受到攻擊而停擺，造成盈餘嚴重損失或客戶的信心受損，也可能導致您公司的獲利率下降。當評估安全成本時，除了要考量IT功能損失的成本以外，也應該包括駭客攻擊所引發的間接成本。

本文針對安全性所做的弱點、風險及暴露分析，可讓您了解安全性與可用性間的取捨，是所有網路環境的電腦系統所必須面對的。這份手冊列出 Windows Server 2003 和 Windows XP 中主要可用的安全性對策、他們處理的安全性弱點，以及實作時每一項潛在可能發生的負面影響。

接著在這份手冊中，提供了在三個常見的企業環境中，補強這些系統的特定建議。第一個環境，是必須支援舊的作業系統一如 Windows 98—的環境；第二個是只包含 Windows 2000 或以上的作業系統；第三個則是安全性需求極高，甚至為了達到最高度的安全性，可以犧牲重要的功能性與管理能力作為交換的系統環境。這三個環境在這份手冊中分別以舊版用戶端 (Legacy Client)、企業用戶端 (Enterprise Client)、高安全性 (High Security) 稱之。我們盡力使得這些資訊有很好的組織及讓大家容易取得，讓您可以迅速找出並決定哪種設定值是最適合您的組織電腦的。雖然這份手冊是針對企業級客戶而寫，但大多數內容對任何規模的組織都適用。

為了從本文得到最大效益，您需要閱讀整份手冊。您也可以參閱配搭的手冊《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》。它可以從 <http://go.microsoft.com/fwlink/?LinkId=15159> 這網址下載。本手冊的製作小組，希望您覺得這份文件所含內容有用、具資訊性、而且是有趣的。

誰應該讀這份手冊

這份手冊主要是針對那些負責應用程式或基礎架構開發的規劃階段，及部署 **Windows Server 2003** 的顧問、安全性專業人員、系統結構師和 IT 專業人員所撰寫的。這些角色包括了以下這些共同的工作描述：

- 結構師和規劃師，負責驅動他們組織中用戶端結構的事物。
- IT 安全性專業人員，其唯一的重心是在他們組織中提供跨平台的安全性。
- 商業分析師與商業決定者 (BDMs)，依賴用戶端支援關鍵性的商業目標與需求。
- Microsoft 服務和其協力廠商的顧問，他們需要掌握相關與有用資訊的詳細資源，以服務企業客戶與協力廠商。

取得安全並保持安全

在 2001 年十月，Microsoft 發起一個名為「策略科技保護計畫」(Strategic Technology Protection Program，簡稱為 STPP)。這計畫的目標就是整合以安全性為焦點的 Microsoft 的產品、服務與支援。Microsoft 視這個維護安全環境的過程為兩個相關的階段，那就是「取得安全(Get Secure)」與「保持安全(Stay Secure)」。

取得安全

第一階段叫做「取得安全(Get Secure)」。為了幫助您的組織達到適當的安全等級，這份手冊中的建議是幫助您保護現有及未來電腦系統安全而設計的。

保持安全

第二階段是「保持安全(Stay Secure)」。創造最初的安全性環境是一回事；然而，待您的環境建立好並開始運轉，能夠長期保持環境安全，採取預防措施來防禦安全性威脅，以及情況真的發生時如何有效地應對，則完全是另一回事。

這份手冊的範圍

這份手冊的重點在於如何讓您組織中執行 Windows Server 2003 的電腦創造並維護具安全性的環境。本文內容解釋在不同階段中要如何保護手冊中所定義的三種環境，以及對每一種環境，根據用戶端的依賴關係，提出伺服器設定值的處方。這邊所指的三種環境是舊版用戶端 (Legacy Client)、企業用戶端 (Enterprise Client)、高安全性 (High Security)。

- 舊版用戶端的設定值，是設計用在 Microsoft Active Directory® 的網域和其成員伺服器中，其中網域控制器是執行 Windows Server 2003，而用戶端則是執行 Microsoft Windows® 98，Windows NT 4.0 或以上。
- 企業用戶端的設定值，是設計用在 Active Directory 網域和其成員伺服器，其中網域控制器是執行 Windows Server 2003，而用戶端執行的是 Windows 2000，Windows XP 或以上。
- 高安全性的設定值，是設計用在 Active Directory 網域和其成員伺服器，其中網域控制器是執行 Windows Server 2003，而用戶端執行的是 Windows 2000、Windows XP 或以上。但是高安全性的設定值有許多限制，以致於可能很多應用程式不能作用。因此，伺服器的效能將受到一些影響，且管理伺服器也將面臨極大的挑戰性。

這份指引是針對一組不同的伺服器角色。文中所提供的對策及工具是假設每一個伺服器只有一個單一角色；如果您需要把環境中一些伺服器角色合併，您可以用這手冊所附的安全範例來修改，來讓服務與安全性選項的組合設定能夠適合擁有多重角色的伺服器。本手冊所涵蓋的角色包括了：

- 網域控制器。
- 基礎架構伺服器。
- 檔案伺服器。
- 列印伺服器。
- 網際網路資訊服務 (IIS) 伺服器。
- 網際網路驗證服務 (IAS) 伺服器。
- 憑證服務 (Certificate Services) 伺服器。
- 防禦 (Bastion) 主機。

本手冊所建議的設定值是經過完整的測試，測試的實驗室環境包含以上所描述的：舊版用戶端，企業用戶端，和高安全性。這些設定值已在實驗室經證實無誤，但是，很重要的是在您自己實驗室中所測試的設定是要能夠精準代表您的生產環境的。您很有可能需要對手冊中所描述的安全範例和手動程序作一些修改，才能夠讓您所有的商業應用程式能如預期地作用。詳細的資訊提供於配合使用的手冊，《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》。可以從這網址 <http://go.microsoft.com/fwlink/?LinkId=15159> 下載，這文件所提供的資訊可讓您能評估每一個對策，並決定哪些是適合您組織的獨特環境和商業需求。

內容概觀

這份 Windows Server 2003 安全性手冊 包含了十二章。每一章都建立端對端的解決方案過程，這是實作及保護您環境中 Windows Server 2003 的安全性所必須具備的。前面幾章主要在描述如何建構安全性基礎來補強您組織中的伺服器，其他的章節則針對每一個伺服器角色獨特的程序作說明。

第一章：簡介 Windows Server 2003 安全性手冊

本章介紹這份 Windows Server 2003 安全性手冊，並包含對每一章的簡要概觀。

第二章：設定網域基礎架構組態

本章解釋網域環境的建構可以作為保護 Windows Server 2003 基礎架構的基礎。首先，這章內容焦點放在網域等級的安全性設定與對策。對 Microsoft Active Directory 服務的設計，組織單位 (OU) 的設計，與網域原則有更深入的描述。

接下來，會以保護網域環境安全為觀點，解釋第一章中提到的舊版用戶端，企業用戶端，和高安全性環境。這可提供您組織一個革新的願景，使您的組織能夠在網域基礎架構中，朝向一個更安全的環境發展。

第三章：建立成員伺服器基礎

本章解釋安全性範例設定和其他的對策，主要是針對這份手冊所定義的三個環境其中所涵括的伺服器角色。本章大半焦點在於建立一個成員伺服器基礎原則 (Member Server Baseline Policy, 簡稱為 MSBP) 來強化稍後對於伺服器角色的補充建議所作的討論。

本章所選擇的建議，是為了使公司能安全地部署對 Windows Server 2003 系統強力推薦的設定組態，因為它們同時適用於現有與新建的系統。Windows Server 2003 中預設的安全組態已經過研究與測試，但本章的建議則是為了提供比預設的作業系統設定值更高的安全性。在某些情況下，若要提供支援舊版用戶端，我們建議使用比 Windows Server 2003 的預設值限制為少的設定組態。

第四章：補強網域控制器

網域控制器伺服器的角色是在保護任何執行 Windows Server 2003 電腦的 Active Directory 環境安全上，扮演最重要的角色之一。任何網域控制器的失敗或妥協，都意味著那些依賴網域控制器進行驗證，執行群組原則，以及集中式輕量型目錄存取通訊協定 (central lightweight directory access protocol, 簡稱為 LDAP) 目錄的用戶端、伺服器和應用程式的損毀。

這一章概要性的說明網域控制器必須存放於真正安全的位置，且只有合格的管理人員能夠存取的。把網域控制器儲存在不安全的地方一例如分公司一便可能引發不必要的風險，同時，本章大部分都花在解釋建議網域控制器群組原則背後所隱含的安全性考量。

第五章：補強基礎架構伺服器

在這一章中，基礎架構伺服器角色被定義為「動態主機控制通訊協定」(Dynamic Host Control Protocol, 簡稱為 DHCP) 伺服器，或是「Windows 網際網路命名服務」(Windows Internet Name Service, 簡稱為 WINS) 伺服器。本章也詳細點出您系統環境中的基礎架構伺服器，可從不套用「成員伺服器基礎原則」(Member Server Baseline Policy, 簡稱為 MSBP) 的安全設定值獲益的地方。

第六章：補強檔案伺服器

本章的重點在於檔案伺服器角色，以及委派給它的補強伺服器所可能發生的相關困難。這些伺服器最基本的服務需要 Windows 的網路基本輸入系統 (NetBIOS) 相關的通訊協定。伺服器訊息區塊 (Server Message Block, 簡稱為 SMB) 和共同網際網路檔案系統 (Common Internet File System, 簡稱為 CIFS) 通訊協定也是用來提供給未經驗證的使用者豐富資訊使用的，然而通常在高安全性的 Windows® 環境中，我們不建議使用。本章也詳細說明檔案伺服器若不套用 MSBP 的安全設定值，可能獲得的好處。

第七章：補強列印伺服器

列印伺服器是這一章的焦點。同樣的，這些伺服器最基本的服務都需要使用到 Windows NetBIOS 相關的通訊協定。SMB 和 CIFS 通訊協定同樣可以提供這個伺服器角色豐富的資訊給未經驗證的使用者，然而通常在高安全性的 Windows 環境中，我們建議停用。此外，本章還會說明列印伺服器的安全設定值若不套用 MSBP，而能夠加以補強的地方。

第八章：補強 IIS 伺服器

這一章概述 Web 網站和應用程式能夠擁有完整的安全性，是來自於整個 IIS 伺服器 (包括每個在這 IIS 伺服器上執行的 Web 網站和應用程式) 在您的環境中能夠受到用戶端電腦的保護。Web 網站和應用程式也必須能夠受到在同一台 IIS 伺服器上執行的其他 Web 網站和應用程式的保護。本章也詳細說明卻使您環境中 IIS 伺服器間的區別性能夠達成的方法。

預設值並沒有將 IIS 安裝於 Microsoft Windows 伺服器系統家族成員中。當 IIS 初始安裝時，是安裝在一個高度安全、「鎖定」的模式下。舉例來說，IIS 的預設值是只針對靜態內容提供服務的。一些功能像是 Active Server Pages (ASP)、ASP.NET、Server-Side Includes、WebDAV 發行，還有 Microsoft FrontPage® 伺服器延伸都必須經由系統管理員透過「網際網路資訊服務管理員」(Internet Information Service Manager，簡稱為 IIS Manager) 中的「網站服務延伸」(Web Service Extensions) 節點來啟用。

本章的各章節詳細提供了各種補強安全性的設定值，這是您應該在您系統環境中的 IIS 伺服器中做設定的，以增進系統安全性。本章也強調安全性的監視、偵測與反應的重要性，以確保伺服器保有安全性。

第九章：補強 IAS 伺服器

網際網路驗證伺服器 (Internet Authentication Server，簡稱為 IAS) 提供 RADIUS 服務，這是一個以標準為基礎的驗證通訊協定，這設計主要是來確認遠端存取網路的用戶端身份。這一章詳細列出了 IAS 伺服器的安全性設定值若不套用 MSBP，可獲得的好處。

第十章：補強憑證服務伺服器

憑證服務 (Certificate Services) 提供密碼與憑證管理的服務，這是建置您系統環境中伺服器的「公開金鑰基礎架構」(PKI) 所需要用到的。這一章詳細列出憑證服務伺服器的安全性設定值若不套用 MSBP，可獲得的好處。

第十一章：補強防禦主機

防禦主機 (Bastion hosts) 伺服器可以從用戶端透過網際網路存取。在這一章解釋這些系統暴露於未受保護的程度有多大，其極可能被很多故意且完全匿名的使用者攻擊。很多組織並不將他們的網域基礎架構開放到公用部份。因此，本章內容的重點是針對獨立的電腦提供補強性建議。關於防禦性主機的安全性設定值若不套用 MSBP，可獲得的好處，或套用這些設定值於 Active Directory 為基礎的網域環境的方法，本章也將詳述。

第十二章：結論

結論這章主要是在重述在前面章節所討論的重點。

工具與範例

安全性範例、指令碼語言，和其他的工具都囊括於本手冊中，好讓您的企業組織可以輕易地評估、測試，與實作本手冊所建議的對策。安全範例是純文字檔案，可以匯入以網域為基礎的群組原則，或直接套用「安全性組態設定與分析(Security Configuration and Analysis)」嵌入式管理單元。詳細程序在第二章「設定網域基礎架構組態」一節有說明。本手冊所包括的指令碼語言是以NETSH 指令列工具及用於測試中所建議的對策的測試指令碼語言來導入 IPSec 封包篩選器。本手冊還包括了一個 Microsoft Excel 工作表叫做 Windows Server 2003 安全性手冊設定，其記載每一個安全範例的設定值。這些工具和範例都在本手冊中附上的自動解壓縮 WinZip 檔案中。當您從壓縮檔案中解出檔案後，以下目錄會在您所指定的位置建立起來：

- Windows Server 2003 Security Guide – 包含您目前正在閱讀的 PDF 檔案文件、測試手冊、傳送手冊，以及與這資料相關聯的支援手冊。
- Windows Server 2003 Security Guide\Tools and Templates – 包含任何伴隨本手冊的項目之子目錄。
- Windows Server 2003 Security Guide\Tools and Templates\Security Guide\Security Templates - 包含本手冊討論到的所有安全範例。
- Windows Server 2003 Security Guide\Tools and Templates\Security Guide\Sample Scripts – 包含所有 IPSec 篩選器指令碼語言的樣本和一個 Excel 工作表，它包含了所有這手冊中討論到的傳輸對應。
- Windows Server 2003 Security Guide\Tools and Templates\Security Guide\Checklists – 包含對每一個伺服器角色特定的檢查清單。
- Windows Server 2003 Security Guide\Tools and Templates\Test Guide – 包含測試手冊相關的工具。
- Windows Server 2003 Security Guide\Tools and Templates\Delivery Guide – 包含與傳送手冊相關的工具。

技術與預備

下列的知識與技術是在企業組織中，負責安裝的 Windows Server 2003 以及開發、部署 Windows XP 以及保護系統安全性的管理員或結構師所需預先具備的。

- MCSE 2000 憑證與兩年以上安全性相關的經驗。
- 深入瞭解公司網域和 Active Directory 環境。
- 使用管理工具，包括了 Microsoft Management Console (MMC)、secedit、gpupdate 和 gpreresult。
- 管理群組原則的經驗。
- 在企業環境中開發應用程式和工作站的經驗。

系統需求

使用本手冊中的工具和範例所需要的軟體需求為：

- Windows Server 2003 標準版、Windows Server 2003 企業版或 Windows Server 2003 Datacenter 版。
- 以 Windows Server 2003 為基礎的 Active Directory 網域。
- Microsoft Excel 2000 或以上。

樣式慣例

本手冊使用以下這些樣式慣例和術語。

表 1.1：樣式慣例

項目	意義
粗體字	字元正如所顯示的輸入，包括指令與指令開關。使用者介面指示性的項目文字也是粗體的。
斜體字	需提供特定值的變數替代位置。例如， Filename.ext 可指任何合於討論情況的，合法的檔案名稱。
重要	警示讀者完成工作所必須的補充性資訊。
等寬的字體	程式碼範例。
%SystemRoot%	Windows Server 2003 作業系統安裝的目錄。
注意	警示讀者的補充性資訊。
Screen Para	出現在螢幕上的訊息或指令列的指令以這種字體顯示。

摘要

本章提供保護 Windows Server 2003 安全性所會涉及的主要問題，而手冊中其他章節將深入探討主要構成問題的因素。現在您對這手冊的章節組織已有瞭解，您可以決定是要從頭讀到尾，或是只選擇您最有興趣的章節來閱讀。

然而很重要，要記得若要達到高效率、高成功率、高安全性的作業，是需要對在這手冊中所提到的所有部分(非其中一些部分)作改進。因此，我們強烈建議您閱讀整份手冊，以便能夠利用手冊中想提供給您保護您組織中 Windows Server 2003 安全性的所有資訊。

詳細資訊

下列資訊來源是這份手冊與產品公開發行時，以及保護 Windows Server 2003 安全性極為相關且最新可用資訊。

如需在 Microsoft 公司中的安全性之詳細資訊，請造訪：<http://www.microsoft.com/security>。

如需知道 MOF 可協助您企業的資訊，請造訪：<http://www.microsoft.com/business/services/mcsmof.asp>。

如需 Microsoft 策略科技保護計畫網站的資訊，請造訪：<http://microsoft.com/security/mstpp.asp>。

如需 Microsoft 安全性通知服務的資訊，請造訪：
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp>。

2. 設定網域基礎架構

概觀

本章將使用網域環境的建構來示範如何保護 Microsoft® Windows Server 2003 的基礎架構。

本章會先將重點放在網域層級的安全性設定和對策。這包含了對 Microsoft Active Directory® 設計的高階描述、組織單位 (OU) 設計、群組原則設計和管理群組設計。

本章也說明了在第一章「保護 Windows Server 2003 安全簡介」所提到的舊版(Legacy)、企業(Enterprise)和高度安全性(High Security)三種環境中如何保護 Windows Server 2003 網域環境安全性的方法。這些資訊將替您打好基礎，並提供在網域基礎架構中從老舊環境轉向高度安全性環境的願景。

Windows Server 2003 在出廠時的預設值即已經設定至安全的狀態。為提升本手冊的可用性，本章僅探討與預設值不同的設定。如需所有預設值的相關資訊，請參閱所附的手冊，《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》。

Active Directory 設計

單單探討設計 Active Directory 結構的詳細資訊就足以填滿整本書的篇幅。Active Directory 可讓應用程式尋找、使用和管理分散式運算環境的目錄資源。本節將簡要地探討這些概念來作為本章其他章節的參考架構。

在建立 Active Directory 架構時，您必須仔細地考量環境的安全性界限為何。若能夠妥善規劃組織的安全性委派和實作時間表，便能夠產生更安全的 Active Directory 設計。在這之後，只有發生重大的環境變更，例如購併或組織重組才會需要重新建構。

若您的組織已經有一個 Active Directory 設計，本章可從安全性的觀點，協助您洞悉其好處或潛在問題。

建立 Windows Server 2003 的目錄界限

在Active Directory中存在一些不同的界限類型。這些界限定義了樹系、網域、網站拓樸和權限委派。

這些界限在Active Directory 安裝時會自動產生，但您仍須確認權限界限是否囊括企業組織的需求和原則。管理權限的委派可以非常彈性地取決於企業組織的需求。例如，若要在安全性和管理功能之間維持適當的平衡關係，您可進一步地將權限委派界限切成安全性界限和管理界限。

安全性界限

安全性界限有助於定義組織內不同群組的自發性或隔離。要能夠確保足夠的安全性（這取決於公司的商務界限如何建立），又同時能夠持續地提供紮實的基本功能，並不是很容易的事。

要適當地取得兩者間的平衡，您必須要衡量管理權限的委外及系統環境網路架構其他權限的委派，對您的組織所可能帶的安全性威脅為何。

樹系 vs. 網域安全性界限

樹系是真正的安全性界限。本手冊建議您去建立個別的樹系，而不是建立個別的網域，以提供安全性，來遏止蓄意破壞的系統管理員或者其他的潛在威脅，進而防止惡劣的系統管理員去破壞系統。

網域是 Active Directory 的管理界限。若組織內的人員都很正派，網域界限可替組織內每個網域中的服務和資料提供自發性管理。

但在探討安全性時，我們知道真實世界並不是如此容易就可達到。例如，網域並無法完全隔離惡劣網域系統管理員的攻擊。此等級的隔離只能在樹系層級中取得。

基於此原因，您的組織可能需考慮將目前 Active Directory 設計內的服務和資料的管理控制分開。對於 Active Directory 設計，您需要充分瞭解您的組織在服務自發性和服務隔離、以及資料自發性和資料隔離上的需求。

管理界限

因為分割服務和資料的潛在需要，您必須定義您所需的各種不同管理層級。除了執行您組織特有服務系統管理員外，建議您同時增設下列管理員。

服務管理員

Active Directory 的服務管理員需負責設定與提供目錄服務。例如，服務管理員需維護網域控制器伺服器、控制整個目錄的組態設定，同時也需要負責確保服務的可用性。您組織內的 Active Directory 系統管理員應視為您的服務系統管理員。

在許多狀況中，Active Directory 服務組態是由屬性值所決定。這些屬性值會分別對應儲存於目錄內的個別物件設定值。因此，Active Directory 內的服務系統管理員也是資料系統管理員。根據您組織的需求，底下列出了可能需包含於您 Active Directory 服務設計內的一些其他服務管理員群組：

- 主要負責目錄服務的網域管理群組。
樹系系統管理員負責選擇群組來管理每個網域。因為每個網域系統管理員將被授與高階的存取權限，這些系統管理員必須相當可靠。負責網域管理的群組將透過 Domain Admins 群組和其他的內建群組來控制網域。
- 負責網域名稱系統 (Domain Name System，簡寫為 DNS) 管理的系統管理員群組。
DNS系統管理員群組負責完成 DNS 設計與管理 DNS 基礎架構。DNS系統管理員將透過 DNS Admins 群組來管理 DNS 基礎架構。
- 負責管理 OU的系統管理員群組。
OU 系統管理員將指定群組或個人作為每個 OU 的管理者。每個 OU 系統管理員需負責管理儲存於所指定 Active Directory OU 內的資料。這些群組可控制管理員如何委派，以及如何將原則套用至其OU內的物件。此外，OU 管理員也可建立新的樹狀子目錄，並委派他們所負責 OU 的管理。
- 負責管理基礎架構伺服器的管理員群組。
負責管理基礎架構伺服器的群組需負責管理 Microsoft Windows® Internet Name Service (WINS)、Dynamic Host Configuration Protocol (DHCP)，亦可能需管理 DNS 基礎架構。在某些狀況中，處理網域管理的群組將需管理 DNS 基礎架構，因為 Active Directory 已經跟DNS做整合，並且儲存及在網域控制器上做管理。

資料管理員

Active Directory 資料系統管理員負責管理儲存於 Active Directory 內的資料或連結至 Active Directory 之電腦內的資料。這些系統管理員並不能控制目錄服務的組態或傳輸。資料系統管理員是您組織所建立之安全性群組的成員。有時候 Windows 內的預設安全性群組並不適用於組織內的所有狀況。因此，組織可發展自己的安全性群組命名標準與定義，來符合本身環境的需要。資料系統管理員的每日例行工作包括了：

- 控制目錄中的物件子集合。透過可繼承屬性層級的存取控制，系統可讓資料系統管理員控制特定的目錄區域，但不能控制服務本身的組態。
- 管理目錄中的成員電腦，以及這些電腦上的資料。

注意：在許多狀況中，儲存於目錄內的物件屬性值決定了目錄的服務組態。

概括來說，要讓 Active Directory 服務和目錄結構的擁有者加入樹系或網域的基礎架構，組織必須信賴樹系和所有網域內的所有服務系統管理員。此外，企業安全性程式必須開發標準的原則和程序，以便替系統管理員提供適當的資訊以做篩選。在此安全性手冊的內容中，信賴服務系統管理員意味著：

- 合理地相信服務系統管理員將會尋求企業組織的最大利益。若樹系或網域的擁有者極有可能對組織做出不利的舉動，企業組織就不應加入該樹系或網域。
- 合理地相信服務系統管理員會遵循最佳實施方針，並限制對於網域控制器的實體存取。
- 必須瞭解與接受企業組織可能面臨的風險，包括了：
 - 惡劣的系統管理員 – 受信任的系統管理員也可能變成惡意的系統管理員，因而濫用了他們對於系統所擁有的能力。若您的樹系內有一個惡劣的系統管理員，該系統管理員便可以輕易地從另一個網域中查出另一個系統管理員的安全性識別項 (SID)。接著，該惡劣系統管理員就可使用應用程式設計介面 (API) 工具、磁碟編輯器或偵錯工具，來將竊取來的 SID 加至自身網域內帳戶的 SID 記錄清單內。當惡劣的系統管理員將竊取來的 SID 加至使用者的 SID 記錄之後，再加上他自己的網域，他便取得竊取來的SID 網域管理權限。
 - 被強迫的管理員 – 受信任的管理員可能會被強迫執行一些破壞系統安全性的動作。使用者或管理員可能會對電腦系統的合法管理員進行社交技術，以取得存取系統所需的使用者名稱和密碼。有些組織可以接受來自組織任一單位的惡劣服務管理員所造成的安全性漏洞風險。這些組織可能認為使用共用的基礎架構來進行的協同合作效益及省下的成本大過於冒此安全性風險。不過，有些組織則無法接受這樣的風險，因為安全性漏洞可能造成的潛在問題實在太嚴重了。

可簡化群組原則管理和委派的 OU 結構

雖然此手冊的重點並非 Active Directory 設計，但要透過群組原則來妥善地管理您企業組織的網域、網域控制器和特定的伺服器角色，某些設計資訊是不可或缺的。

OU 除了提供了一個簡單的方式給群組使用者和其他的安全性主角外，它們更提供一個有效的機制來分割管理界限。

此外，根據伺服器角色使用 OU 來提供不同的群組原則物件 (GPO)，也是企業組織的整體安全性架構中不可或缺的一環。

委派管理與套用群組原則

OU 在網域內就只是一個容器。您可藉由在每一個容器上設定特定的存取控制清單 (ACL)，然後將 OU 上的控制權委派給群組或個人。

通常，您可使用 OU 來提供類似於 Microsoft Windows NT[®] 4.0 資源網域所提供的管理功能。您也可建立一個 OU 來包含資源伺服器群組，以供其他使用者管理。如此，這群由其他使用者所組成的群組將可自發地控制特定的 OU，而不需將他們與網域的其他部分隔開。

委派特定 OU 之控制權的系統管理員可能是服務管理員。在較低的授權層級中，控制 OU 的使用者通常為資料系統管理員。

管理群組

建立管理群組可讓系統管理員將使用者叢集、安全性群組或伺服器分割到各個容器中，以進行自發性管理。

例如，位於網域內的基礎架構伺服器便是一例。基礎架構伺服器包含了所有執行基本網路服務的非網域控制器，包括了執行 WINS 和 DHCP 服務的伺服器。所有的 DNS 伺服器都執行於網域控制器上，它們位於網域控制器 OU 內。此範例中的 DNS 伺服器並不被視為基礎架構伺服器。

通常，一個作業群組或基礎架構管理群組將負責維護這些伺服器。使用 OU 可以輕鬆地提供管理能力給這些伺服器。

- 若要建立 OU 來進行管理
 1. 建立一個稱為 Member Servers 的 OU。
 2. 建立一個稱為 Infrastructure 的 OU。
 3. 將所有的 WINS 和 DHCP 伺服器移到 Infrastructure OU 之中。
 4. 建立一個稱為 Infrastructure Admins 的網域安全性群組，並加入適當的網域帳戶。
 5. 執行 Delegation of Control Wizard，以提供 OU 的完整控制設定給 Infrastructure Admins 群組。

下圖提供了這類 OU 的高階檢視圖。

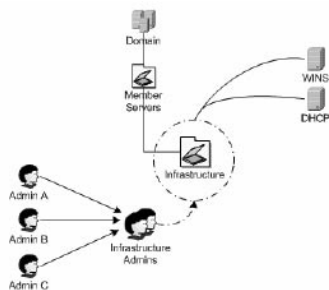


圖 2.1

OU 的管理委派

這只是使用 OU 來提供系統管理分割的眾多方法之一。對於更複雜的組織，請參閱本章後面的「詳細資訊」小節。

執行完此程序之後，Infrastructure Admin 群組應可完整地控制 Infrastructure OU，以及此 OU 內的所有伺服器 and 物件。這為它們進入下個階段做準備，即以群組原則(Group Policy)來保護伺服器角色的安全。

群組原則的套用

您可使用群組原則並委派管理，以套用特別的設定、權限和運作方式到 OU 內的所有伺服器上。透過使用群組原則，而非手動步驟，日後您可輕鬆地更新需要進行任何額外變更的眾多伺服器。

群組原則將以下圖所表示的順序累積與套用。

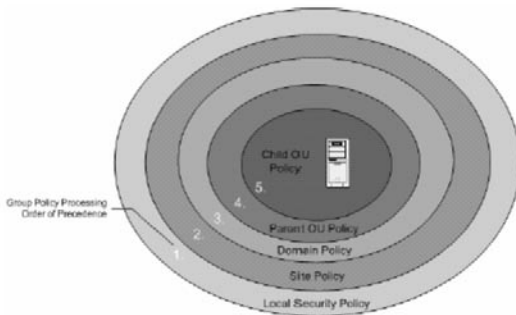


圖 2.2
GPO 套用的階層架構

如上圖所示，原則會先從電腦的本機原則層級開始套用。之後，任何 GPO 將套用於網站層級，接著再套用於網域層級。若伺服器套疊於多個OU內，位於最高層OU的GPO將會先套用。套用GPO的流程會一直持續到 OU 階層架構下層。最後一個套用的GPO是位於包含伺服器物件的子 OU 層級。處理群組原則的優先順序將從最高的 OU (距離使用者或電腦帳戶最遠的 OU) 延伸到最低的 OU (實際包含使用者或電腦帳戶的 OU)。

在套用群組原則時，請記住下列幾點：

- 您必須替具有多個 GPO 的群組原則層級設定 GPO 的套用順序。若多個原則都指定相同的選項，最後套用的原則將有較高的優先權。
- 以 No Override 選項來設定群組原則可防止其他 GPO 蓋過它。

安全性範本

安全性範本是文字型態的檔案。您可使用 Microsoft Management Console (MMC) 的 Security Templates 嵌入式管理單元，或使用記事本等文字編輯程式來變更這些檔案。範本檔的一些區段包含了撰寫於 Security Descriptor Definition Language (SDDL) 之中的特定 ACL。您可在編輯 Microsoft MSDN® 上的安全性範本和 SDDL 時發現更多資訊。

範本管理

在預設狀態下，驗證過的使用者就有權讀取群組原則物件內包含的所有設定。因此，將生產環境所使用的安全性範本儲存到安全的位置，使得只有負責實作群組原則的系統管理員能夠存取的，這是相當重要的。其用意是防止他人擅自變更原始的安全性範本，而不是防止他人檢視 *.inf 檔。為滿足此需求，所有執行 Windows Server 2003 的電腦都會將安全性範本儲存到 %SystemRoot%\security\templates 資料夾內。

不過，此資料夾並沒有在多個網域控制器中複製。因此，您需要指定一個網域控制器來包含安全性範本的主要複本，以免發生範本版本無法有效控管問題。如此，便可確保您能夠修改到相同的一份範本。

管理群組原則與匯入安全性範本

下列程序會將此手冊所包含的安全性範本匯入到本章所建議的 OU 結構內。當您在某個網域控制器上實作下列程序前，務必先將特定的原則檔案 (.inf) 放在環境中的 Windows Server 2003 系統內。

警告：本手冊內的安全性範本是為了增加您環境的安全性而設計的。當您安裝了此手冊所附的範本之後，您企業組織環境中的某些功能可能會消失。甚至可能造成重要的應用程式無法執行。

因此在將這些範本部署到實際執行環境之前，務必徹底地測試它們。請在套用任何新的安全性設定之前，先備份您環境中的每個網域控制器和伺服器。請確認系統狀態亦包含於備份之中，以便讓登錄設定或 Active Directory 物件也可還原。

- 若要匯入 Domain Policy 安全性範本
 1. 在 Active Directory Users and Computers 中，以滑鼠右鍵按一下 Domain，然後選取 Properties。
 2. 在 Group Policy 索引標籤中按一下 New，加入新的 GPO。
 3. 鍵入 Enterprise Client - Domain Policy，接著按 Enter。
 4. 以滑鼠右鍵按一下 Enterprise Client - Domain Policy，接著選取 No Override。
 5. 選取 Enterprise Client - Domain Policy，接著按一下 Edit。
 6. 在群組原則視窗中按一下 Computer Configuration\Windows Settings。以滑鼠右鍵按一下 Security Settings，接著選取 Import Policy。
 7. 在 Import Policy From 對話方塊中移至 \Security Guide\Job Aids，接著連按兩下 Enterprise Client - Domain.inf。

8. 關閉修改過的群組原則。
9. 關閉 Domain Properties 視窗。
10. 在網域控制器之間強迫複製，以透過下列程序讓它們全都套用原則：

- 開啓一個命令提示字元，並使用 `gpupdate.exe` 命令列工具，強迫網域控制器以下列命令重新整理網域原則：`gpupdate /Force`。

11. 在 Event Log 中確認群組原則已成功地下載，並且該伺服器可以與網域中的其他網域控制器互相通訊。

警告：當您建立 Enterprise Client - Domain Policy 時，確認 No Override 選項已啓用，以便將此原則強制套用在整個網域內。這是本手冊中唯一必須啓用 No Override 選項的群組原則。請勿在本手冊指定的其他群組原則中啓用此選項。此外，假使您需要還原 Windows Server 2003 的原始預設值，請勿修改 Windows Server 2003 的預設網域原則 (Default Domain Policy)。

爲確保此新原則的優先順序高過預設的原則，請安排其位置，讓它在 GPO 連結之間具有最高的優先順序。

您可直接修改預設原則來建立新的安全性組態，不過，建立新的群組原則有一個好處 — 若新的群組原則有任何問題，您可以輕鬆地停用它，並讓預設網域原則繼續接手控制。

Gpupdate.exe 是一個命令列工具，當您從批次檔或自動化工作排程器呼叫它時，可用它來自動套用範本與分析系統安全性。它也可動態地從命令列中執行。

重要：此原則應匯入至組織內的任何額外網域之中。不過，您可能經常發現根網域的密碼原則比任何其他網域來得嚴格。您也應小心確保其他會使用此原則的網域是否都有相同的商業需求。由於密碼原則只能設定於網域層級，可能有些商務或合法需求會將一些使用者分配到個別的網域中，其作用只是要在該群組內強制使用更嚴格的密碼原則。

在此手冊定義的三個環境中，其根網域和子網域都使用相同的原則，並搭配每一個相關安全性範本。例如，Legacy Client - Domain.inf、Enterprise Client - Domain.inf、High Security - Domain.inf 檔都用於每一個個別的層級中。您應使用類似上述的程序，來將基礎原則和累加原則套用到後續範本中。

成功的 GPO 應用程式事件

除了透過手動來檢查所有設定，以確認它們已適當地套用至您企業組織內的所有伺服器中之外，事件記錄檔 (Event Log) 內應該也會出現一個事件，好讓系統管理員知道網域原則已成功地下載至每台伺服器上。下列的事件資訊應該連同它自己的唯一事件 ID 編號出現在應用程式記錄檔 (Application Log) 內：

Type: Information

Source ID: SceCli

Event ID: 1704

Description: Security policy in the Group policy objects has been applied successfully.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

若此訊息未在套用網域原則後的幾分鐘內出現，請重新執行 `Gpupdate.exe` 命令列工具來套用網域原則，然後再重新啟動伺服器去強迫下載網域原則。

在預設狀態下，工作站或伺服器的安全性設定每 90 分鐘會重新整理一次，若是在網域控制器上，則為每 5 分鐘重新整理一次。若在這些期間發生了任何變更，您將會看到此事件。此外，這些設定也會每隔 16 小時重新整理一次，不管是否有新的變更。

時間組態

您應確保系統時間是正確的，並且您組織中的所有伺服器都使用相同提供時間的來源。Windows Server 2003 W32Time 服務可替執行於 Active Directory 網域內的 Windows Server 2003 和 Microsoft Windows XP 電腦，提供時間同步化功能。

W32Time 服務可讓 Windows Server 2003 電腦的用戶端時鐘與網域內的網域控制器同步化。要讓 Kerberos 5.0 版的驗證通訊協定以及 NTLMv2 能夠正常運作，這是必要的。要正確地運作，許多 Windows Server 系統元件都有賴正確以及同步化的時間。若用戶端上的時鐘並未同步化，Kerberos v5 驗證通訊協定可能會誤將登入要求解釋成侵入嘗試，並拒絕使用者的存取。

時間同步化提供的另一項重要好處是可以提供您企業中所有用戶端上所發生事件的關聯性。在您系統環境中的用戶端同步化時鐘可確保您一致且依序，正確地分析發生於企業組織中用戶端上的事件是成功還是失敗。

Kerberos 是由麻省理工學院 (MIT) 所發展的一個網路驗證通訊協定。此通訊協定可透過秘密金鑰加密技術，驗證嘗試登入至網路的使用者識別，並將其通訊加密。

W32Time 服務會使用 Network Time Protocol (NTP) 來將時鐘同步化。在 Windows Server 2003 樹系中，

時間將以下列方式進行同步化：

- 在樹系根網域中的主網域控制器 (PDC) 模擬器操作主機是企業組織可信賴的時間來源。
- 在樹系內其他網域中的所有 PDC 操作主機在選取 PDC 模擬器來將其時間同步化時，都遵循網域的階層架構。
- 網域中的所有網域控制器都會將它們的時間同步化，並以其網域內的 PDC 模擬器操作主機作為其傳入時間伙伴。
- 所有的成員伺服器 and 用戶端桌面電腦都使用驗證網域控制器作為其傳入時間伙伴。

為確保時間是正確的，樹系根網域內的 PDC 模擬器可與外部的 NTP 時間伺服器同步化。不過，若要如此做，您可能需要將防火牆上的連接埠開啓。NTP 使用 UDP 連接埠 123。在此之前，請您先權衡其好處，以及進行這些組態變更可能帶來的安全性風險。

- 將內部的時間來源和外部的時間來源同步化
 1. 開啓一個 Command Prompt (命令提示字元)。
 2. 鍵入下列資料，此處的 PeerList 是一個由逗點隔開的清單，裡面包含了您要的時間來源的 DNS 名稱或 Internet protocol (IP) 位址：
`w32tm /config /syncfromflags:manual /manualpeerlist:PeerList`
 3. 要更新類型：
`w32tm /config /update。`
 4. 檢查事件記錄檔。若電腦無法連到伺服器，此程序將會失敗，並且事件記錄檔中會寫入一個項目。

此程序最常見用途是將內部網路的可信賴時間來源與極精確的外部時間來源同步化。但這程序可執行於任何一台執行 Windows XP 或 Windows Server 2003 系統成員的電腦上。

在許多狀況中，並非所有的伺服器時間都需要與外部來源同步化，它們只要與同一個內部來源同步化即可。

若您網路上的電腦執行的是 Windows 98 或 Windows NT 4.0 作業系統，那您可在登入指令碼中使用下列命令，來將這些機器的時鐘同步化，此處的 <timecomputer> 是網路上的網域控制器：

```
net time \\<<timecomputer> /set /yes
```

執行此命令可將這些電腦裡的時鐘和網域內其他電腦的時時鐘同步化。

注意：如需精確的記錄檔分析，不是執行 Windows 作業系統的網路電腦也應將其時鐘和 Windows Server 2003 PDC 模擬器同步化。

基礎伺服器角色組織單位

您可將上一個管理組織基礎架構伺服器的範例加以擴充，再加入公司基礎架構內的其他伺服器和服務。目的是建立一個可涵蓋所有伺服器的群組原則，同時並確保位於 Active Directory 內的伺服器可滿足您環境的安全性標準。

這類涵蓋您環境所有伺服器的群組原則可構成您企業中所有伺服器標準設定的一致基礎。此外，OU 結構和群組原則的應用則必須提供更細微的設計，以便替組織內的特定伺服器類型提供安全性設定。例如，Internet Information Server (IIS)、檔案、列印、Internet Authentication Server (IAS) 和認證服務都是組織中可能需要唯一群組原則的一些伺服器角色。

成員伺服器基礎原則

建立伺服器角色 OU 的第一步是建立一個基礎原則。其作法是建立一個基礎安全性範本，並將它匯入群組原則內。本安全性手冊內所包含的 Enterprise Client - Member Server Baseline.inf 檔就可提供這樣的功能和指引。根據第一章「Introduction to the Windows Server 2003 Security Guide」所探討的企業組織相容性需求，可作為企業用戶端不同層級的安全性參考。

將此 GPO 安全性範本連結至 Member Servers OU。Enterprise Client -Member Server Baseline.inf 安全性範本，便可將基礎群組原則的設定套用至 Member Servers OU 任一的伺服器中，以及子 OU 中的任何伺服器。為了簡化起見，本章其他的範例將使用企業用戶端這個安全性層級。關於成員伺服器基礎原則將於第三章「建建成員伺服器基礎」中探討。

基礎群組原則應為您定義組織內的所有伺服器的設定。請儘可能的提高基礎群組原則的限制，並將需要和此原則有所區別的任何伺服器分割成個別的伺服器-特定OU。

伺服器角色類型和組織單位

延續上述的範例，您可替就基礎架構伺服器原則不斷變更的部份，建立個別的原則。並將必要的設定放入名為 Enterprise Client - Infrastructure Server.inf 的安全性範本中，以確保基礎架構服務可正常運作，並可透過網路來存取。

將此 GPO 基礎架構範本連結至 Infrastructure OU。最後，使用 Restricted Groups 設定將下列三個群組加到 “Enterprise Client:Infrastructure Server Policy” 的 Local Administrators 群組內：「Domain Administrators」、「Enterprise Administrators」與「Infrastructure Administrators」。

此流程將如下圖所示。

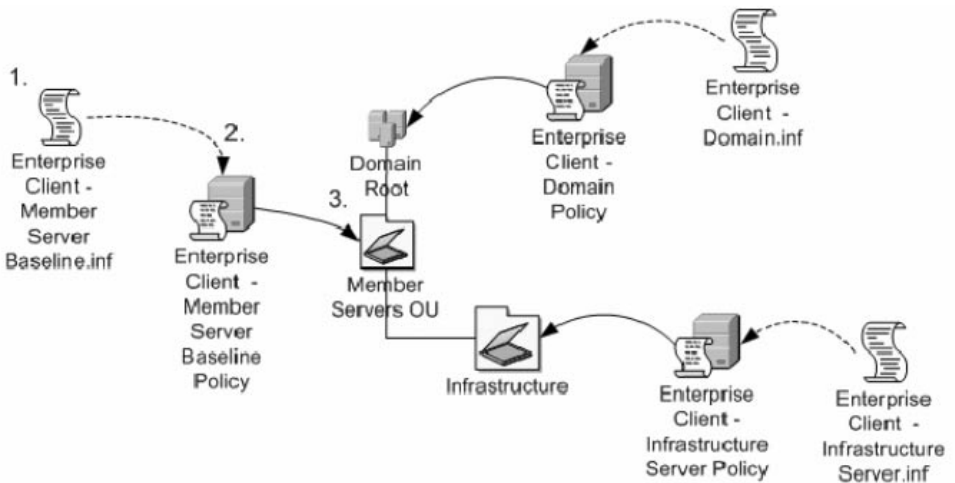


圖 2.3
設定累加的群組原則

如同先前所述，這只是建立 OU 結構來部署 GPO 的眾多可能方式之一。如需建立 OU 來實作群組原則的詳細資訊，請參閱 Microsoft TechNet 文件 “How to Deploy Active Directory”，網址為：
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/AD/windows2000/deploy/depovg/add.asp>。

此安全性手冊定義了多個伺服器角色。下表包含了依循上述流程來增加這些角色安全性的範本。

表 2.1：Windows Server 2003 角色

伺服器角色	描述	安全性範本
Windows Server 2003 網域控制器	包含 Active Directory 網域控制器的群組。	Enterprise Client - Domain Controller.inf
Windows Server 2003 成員伺服器	身為網域成員、並且位於成員伺服器 OU 內部或底下的所有伺服器。	Enterprise Client - Member Server Baseline.inf
Windows Server 2003 檔案伺服器	包含鎖定之檔案伺服器的群組。	Enterprise Client - File Server.inf
Windows Server 2003 列印伺服器	包含鎖定之列印伺服器的群組。	Enterprise Client - Print Server.inf
Windows Server 2003 基礎架構伺服器	包含鎖定之 DNS、WINS 和 DHCP 伺服器的群組。	Enterprise Client - Infrastructure Server.inf
Windows Server 2003 IAS 伺服器	包含鎖定之 IAS 伺服器的群組。	Enterprise Client - IAS Server.inf
Windows Server 2003 認證服務伺服器	包含鎖定之認證授權 (Certificate Authority，簡寫為 CA) 伺服器的群組。	Enterprise Client - CA Server.inf
Windows Server 2003 防禦主機 (Bastion Hosts)	包含 Internet facing 伺服器的群組。	High Security - Bastion Host.inf
Windows Server 2003 IIS 伺服器	包含鎖定之 IIS 伺服器的群組。	Enterprise Client - IIS Server.inf

所有累加的範本檔都應套用至成員伺服器 OU 底下的 OU。基於此理由，這每一個較低層級的 OU 都要您同時套用 Enterprise Client - Member Server Baseline.inf 檔和特定的累加檔到它們上面，以定義組織內的每個角色。

每一個伺服器角色的安全性需求都不相同。後面的章節將會詳細地探討每個角色的適當安全性設定。

重要：此手冊將確保執行 Windows Server 2003 的電腦會執行特別定義的角色。若您組織中的伺服器不符合這些角色，或您擁有多用途的伺服器，可使用此處定義的設定作為建立您自己安全性範本的方針。不過，請記住您伺服器所執行的功能越多，受駭客攻擊的機會就越大。

下圖說明支援這些已定義伺服器角色的最後的 OU 設計圖。

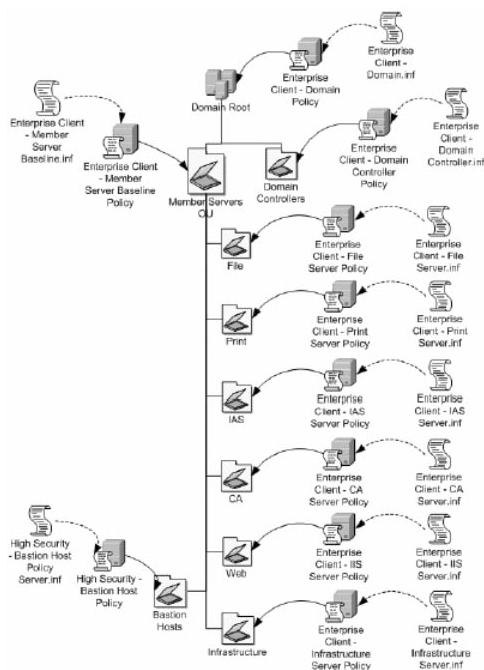


圖 2.4
OU 設計的範例

OU、GPO 和管理群組設計

以上所建議的 OU 和群組原則建立了一個基礎或全新的環境，可替執行 Windows Server 2003 的電腦重建公司現有的 OU 結構。此外，管理員可使用他們預先定義的管理界限來建立個別的管理群組。下表說明了這些群組和他們所管理 OU 的關係。

表 2.2：OU 與管理群組

OU 名稱	管理群組
Domain Controllers	Domain Engineering
Member Servers	Domain Engineering
Infrastructure	Operations
File	Operations
Print	Operations
IAS	Domain Engineering
CA	Enterprise Admins
Web	Web Services

每個管理群組都建立於環境中，作為子網域內的全域群組。

網域工程已使用對應的 GPO，並將每個管理群組加到適當的受限群組內。以上所建立的管理群組只會成為 OU 內電腦的 Local Administrators 群組成員，這裡面包含了與其工作功能相關的電腦。

最後，網域工程師會在每個 GPO 上設定權限，如此只有網域工程群組內的管理員可編輯它們。

在預設狀態下，新的 OU 結構會從其父容器中繼承許多安全性設定。對於每個 OU，請清除「允許從父系容器中將繼承使用權傳播到這個物件及所有子物件中(Allow inheritable permissions from parent to propagate to this object and all child objects)。」核取方塊。

- 若要清除 Allow Inheritable Permissions 選項
 1. 開啟 Active Directory Users and Computers。
 2. 按一下 View 來選取 Advanced 檢視，然後按一下 Advanced Features。
 3. 以滑鼠右鍵按一下適當的 OU，接著按一下 Properties。
 4. 按一下 Security 索引標籤，接著按一下 Advanced。
 5. 清除「允許從父系容器中將繼承使用權傳播到這個物件及所有子物件中。包括特別在此處有定義者。(Allow inheritable permissions from parent to propagate to this object and all child objects. Include these with entries specifically defined here)」核取方塊。

請移除管理員先前加入的任何多餘群組，並加入可對應到每個伺服器角色 OU 的網域群組。並保留 Domain Administrators 群組的 Full Control 設定。

您並不需要以特別的順序來執行建立這些 OU 的工作，但它們之間有一些明顯的相依性。例如，在您委派不同 OU 的控制權給網域群組之前，這些網路群組必須是存在的。底下的清單定義了實作這些工作的建議順序：

1. 建立 OU 結構。
2. 將電腦移到適當的 OU 內。
3. 建立管理群組。
4. 加入適當的網域帳戶到管理群組內。
5. 將每個 OU 的管理委派給適當的網域群組。
6. 在欲套用群組原則的 OU 中建立它們。
7. 依需要將每個群組原則連結至任何額外的 OU。
8. 匯入適當的安全性範本到每個 GPO 內。
9. 在每個 GPO 上設定權限，以便讓適當的網域群組可控制它們。
10. 將適當的網域群組加到每個 GPO 的受限群組 (Restricted Groups) 中。
11. 測試與修改群組原則。

網域原則

您可將群組原則的安全性設定套用到企業組織中的多個不同層級中。以上所探討的基礎環境是使用群組原則來將設定套用到底下的三階層網域基礎架構中：

- 網域階層。用來滿足必須強制套用至網域中所有伺服器的常見安全性需求，例如帳戶和密碼原則。
- 基礎階層。用來滿足網域基礎架構內所有伺服器共通的特定伺服器安全性需求。
- 角色特定階層。用來滿足特定伺服器角色的安全性需求。例如，基礎架構伺服器的安全性需求就和執行 Microsoft Internet Information Services (IIS) 的伺服器需求不同。

本章底下的章節只會詳細地討論網域層級的原則。大部份我們所討論到的網域安全性設定都是用於使用者帳戶和密碼。請記住，在檢視這些設定和建議時，所有的設定都可用於網域界限內的每個使用者。

網域原則概觀

群組原則相當強大，因為它可讓管理員設定標準的網路電腦。透過讓管理員同時在網域或網域子集中的所有電腦上進行安全性變更，GPO 可替任何企業提供組態管理解決方案的重要部分。

本節在安全性設定上提供了詳細的說明，可讓您用來增強 Windows Server 2003 的安全性。此處我們亦提供一個表格來說明每個設定的安全性目標，以及達到每個目標所需的組態。這些設定將根據它們出現在 Windows Server 2003 Security Configuration Editor (SCE) 使用者介面中的方式，來切割成不同的類別。

您可同時以群組原則來套用的安全性變更的類型包括了：

- 在檔案系統上修改權限。
- 在登錄物件上修改權限。
- 在登錄中變更設定。
- 變更使用者權限設定。
- 設定系統服務。
- 設定稽核與事件記錄檔。
- 設定帳戶與密碼原則。

帳戶原則

在本手冊所詳述三個環境的網域原則中，只有帳戶原則比較有相關（帳戶原則包括了密碼原則（Password Policy）、帳戶鎖定機制（Account Lockout Policy）和 Kerberos 原則等安全性設定）。密碼原則提供一個方法來在高度保護的環境密碼中設定其複雜度和變更排程。帳戶鎖定機制可讓您追蹤不成功的密碼登入記錄，必要時會啟動帳戶鎖定。Kerberos 原則適用於網域使用者帳戶。它們決定了 Kerberos 的相關設定，例如票證的存留期和強制使用。

密碼原則

經常變更的複雜密碼可減少密碼被成功攻擊的可能性。密碼原則的設定控制了密碼的複雜度和存留期。本節將討論每個特定的密碼原則設定，以及這些設定與下列三個環境的關係：舊版用戶端、企業用戶端和高安全性。

嚴格訂定密碼的長度和複雜度，未必意味著使用者和管理員需要使用強式密碼。雖然透過啓用密碼原則，系統的使用者可滿足系統所定義密碼的技術複雜度需求，但仍需要額外的強式公司安全性原則來變更密碼的誤用習慣。例如，**Breakfast!** 也許可滿足所有密碼複雜度的需求。但這並非很難破解的密碼。

只要您認識建立密碼的人，就可以根據他偏好的食物、汽車或電影來臆測其密碼。教育使用者選擇強式密碼的公司安全性方案策略之一，就是製作海報來說明不良的密碼，並將它張貼在公共區域，例如飲水機或影印機旁邊。您的組織應設定建立強式密碼的安全性方針，包括了：

- 避免使用字典內的單字、常見或巧妙誤拼的單字、外國單字。
- 避免使用包含一個數字的遞增式密碼。
- 避免在密碼之前或之後加上一個數字。
- 避免使用他人只要看看您的桌面就猜得到的密碼 (例如寵物名稱、運動隊伍、家族成員)。
- 避免使用正在流行的單字。
- 勿將密碼視為單字 — 應視為秘密的代碼。
- 強制使用需要兩隻手方能在鍵盤上鍵入的密碼。
- 強迫所有的密碼都使用大寫和小寫的字母、數字和符號。
- 強迫使用空白字元和必須按下 **Alt** 鍵方能產生的字元。

以上的方針也應該用於您組織內的所有服務帳戶密碼底下的章節包括了適用此手冊所定義三個安全性環境的密碼原則建議。這些值均設定於：

Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy

Enforce password history

表 2.3：設定值

網域成員預設值	舊版用戶端	企業用戶端	高安全性
記住 24 組密碼	記住 24 組密碼	記住 24 組密碼	記住 24 組密碼

此 Enforce password history 設定決定了使用者帳戶必須用過多少個唯一的新密碼之後，才能重複使用舊的密碼。此數值必須介於 0 到 24 個密碼之間。Windows Server 2003 的預設值為最大值，24 組密碼。此原則設定值可讓管理員確認舊的密碼不會持續地重複使用，藉此來增強安全性。要維持密碼記錄的有效性，您亦可設定 Minimum password age，以防止密碼立即變更。此組合可讓使用者很難重複使用密碼，不管是意外或故意。

因為重複使用密碼很容易出現安全性漏洞，但將此設定設得太小，就會導致使用者持續地重複使用少數密碼，因此本手冊所定義的所有環境都採用一樣的建議設定值。此外，對於包含舊版用戶端的環境而言，設定此數值並不會產生任何已知的問題。

Maximum password age

表 2.4：設定值

網域成員預設值	舊版用戶端	企業用戶端	高安全性
42 天	42 天	42 天	42 天

您可設定 Maximum password age 設定值，替您的環境設定所需的密碼過期天數。此設定的預設值可從 1 到 999 天。此原則設定值定義了想要破解密碼的駭客有多少時間，可在密碼過期之前用來存取網路上的電腦。經常變更密碼是一個防止密碼洩漏的方法。此設定的預設值為 42 天。

只要時間和運算能力足夠的話，大多數的密碼都還是破解得開來；密碼越常變更，駭客可用來破解密碼的時間就越少，新的密碼一建立，之前破解舊密碼所花的功能就都白費了。不過，此數值設得越小，需要服務台支援的電話數就可能變得很多。為了讓公司系統環境的安全性和可用性需求間能夠取得平衡點，您可在舊版用戶端和企業用戶端內增加此設定。上述建議的數值可確保密碼定期地循環，進而增加密碼的安全性。此外，我們所建議的數值亦可防止使用者太過頻繁地變更其密碼，以致於記不住密碼。

Minimum password age

表 2.5：設定值

網域成員預設值	舊版用戶端	企業用戶端	高安全性
1 天	2 天	2 天	2 天

Minimum password age 設定值決定了密碼至少須使用幾天，使用者才能變更它。此設定值的數值範圍介於 0 到 999 天。將它設成 0 可讓您立即變更密碼。此設定的預設值為 1 天。

除非您將 Maximum password age 設定值設成 0 (這代表密碼永遠不會過期)，否則 Minimum password age 設定值都必須小於 Maximum password age 設定值。在此狀況中，Minimum password age 可設成介於 0 到 999 的任何數值。

若您希望 Enforce password history 有效，則必須將 Minimum password age 設成大於 0 的數值。若無最小的密碼期限，使用者可重複地循環選用密碼，直到取得先前的偏好密碼。

此處將此設定從預設值改成 2 天，因為當 Enforce password history 設定值也設得很低時，此設定所帶來的限制將可防止使用者不斷地重複使用相同的密碼。若 Minimum password age 保持為 1 天，而 Enforce password history 設成 2 組密碼，使用者只需等兩天，即可重複採用舊的偏好密碼。此設定值可確保使用者必須等待兩整天，才能變更密碼。

預設值並未採用上述的建議，這是為了讓管理員可替使用者指定一密碼，接著在使用者登入時，要求使用者變更管理員所定義的密碼。若密碼記錄設成 0，使用者並不需要選擇新的密碼。基於此原因，Enforce password history 的預設值設成 1。它也可防止使用者快速地設定 24 組新的密碼，以規避 Password history setting 的限制。

Minimum password length

表 2.6：設定值

網域成員預設值	舊版用戶端	企業用戶端	高安全性
7 字元	8 字元	8 字元	12 字元

Minimum password length 設定值可確保密碼至少包含指定的字元數。長密碼 — 至少八個字元 — 通常比短密碼來得安全。透過此原則設定，使用者不能使用空白的密碼，並且必須建立某個字元長度的密碼。此設定的預設值為 7 個字元，但建議您使用 8 字元的密碼，因為它長到足以提供某個等級的安全性，但也不至於長到讓使用者記不住。此設定可針對常用的字典式 (Dictionary) 和暴力式 (Brute Force) 攻擊提供大量的防禦。

字典式攻擊指的是以嘗試錯誤來取得密碼的方法，駭客會使用單字清單中的所有項目。暴力式攻擊指的是透過嘗試所有可能的值，來取得密碼或其他加密文字的方法。暴力式密碼攻擊的可行性取決於密碼的長度、潛在字元集的大小以及駭客可運用的運算能力。

此手冊建議您將高安全性環境中的密碼長度設成 12 個字元。

密碼將在通過單向的雜湊演算法之後，會儲存於 Security Accounts Manager (SAM) 資料庫或 Active Directory 之中。這類演算法不可反向執行。因此，分辨您是否擁有正確密碼的唯一方式是讓它通過相同的單向雜湊演算法，並比較其結果。字典式攻擊會在加密過程中比對整本字典，以找出相同的單字。這是一個簡單但極為有效的作法，可找出以常見單字，例如 “password” 或 “guest”，作為帳戶密碼的使用者。

若密碼為七個字元或更少字元，LM Hash 的後半部分會解析出特定數值，它可讓破解者知道密碼比八個字元來得短。要求密碼至少包含八個字元可增強LMHash的安全性 (即使是較弱的 LMHash)，因為在處理較長的密碼時，破解者需要解密每個密碼的兩個部分，而非一個。因為您可平行地攻擊 LM 雜湊的兩個部分，LM 雜湊的第二部分只有 1 個字元的長度；暴力式攻擊只需幾個毫秒即可破解它，因此除非它是 ALT 字元集，否則功效並不大。

此外，密碼內的每個額外增加一個字元，其複雜度會呈現指數式的增加。例如：七字元的密碼將有 26^7 或 1×10^7 的可能組合。將大小寫視為不同的七字元文字型密碼將有 52^7 種組合。將大小寫視為不同、但不含標點符號的七字元文數字型密碼將有 62^7 種組合。若每秒鐘嘗試 1,000,000 次，只需 48 分鐘即可破解。

八字元的密碼將有 26^8 或 2×10^{11} 的可能組合。乍看之下，此數字好像很驚人。不過，就許多密碼破解公用程式的能力 — 每秒嘗試 1,000,000 次而言，亦只需 59 小時即可嘗試所有可能的密碼。請記得，若使用 ALT 字元和其他的特殊鍵盤字元，例如 ! 或 @，這些時間將會大幅增加。

基於此原因，我們不建議您使用較短的密碼來取代較長的密碼。不過，要求太長的密碼，可能會造成密碼輸入錯誤的情況增加，進而增導致帳戶被鎖住的數目大增，服務台電話的頻率也因此大幅增加。

再者，要求過長的密碼也可能會降低組織的安全性，因為使用者極可能需寫下密碼，以防止忘記。

Password must meet complexity requirements

表 2.7：設定值

網域成員預設值	舊版用戶端	企業用戶端	高安全性
啟用	啟用	啟用	啟用

Password must meet complexity requirements policy 選項會檢查所有的新密碼，確保它們符合強式密碼的基本要求。

在建立密碼時，系統會強制套用複雜度要求。Windows Server 2003 原則規則並無法直接修改。不過，您可建立新版的 passfilt.dll 以套用一組不同的規則。如需 passfilt.dll 的原始碼，請參閱 Microsoft 知識庫文件 151082：“HOW TO:Password Change Filtering & Notification in Windows NT”。

事實上，和 8 字元的密碼相比，20 個或更多字元的密碼有時反而更容易讓使用者記住 — 也更安全。底下列出了一個 27 字元的密碼：I love cheap tacos for \$.99。這類密碼事實上是一個通關片語，對使用者而言，它可能比 P@55w0rd 這類較短的密碼來得好記。

使用此建議值，並將 Minimum password length 設成 8，將可包含鍵盤中的大小寫字母和數字，因此可用字元從 26 變成 62 個。八字元的密碼將擁有 2.18×10^{14} 的可能組合。若每秒嘗試 1,000,000 次，您需要花上 6.9 年才能試完所有可能的排列組合。透過搭配使用這些設定，他人將很難進行暴力式攻擊。基於這些理由，此數值成為本手冊所定義的三種系統環境的建議密碼。

Store password using reversible encryption

表 2.8：設定值

網域成員預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	停用	停用

Store password using reversible encryption 的安全性設定決定了作業系統是否使用可逆式加密 (Reversible Encryption) 來儲存密碼。

此原則可讓使用通訊協定的應用程式基於驗證的用途，要求使用者的密碼。使用可逆式加密來儲存的密碼在擷取時，會比不使用此選項來儲存的密碼容易得多，因此也較為脆弱。基於此理由，除非應用程式的需求高過保護密碼資訊的需求，否則絕對不要啓用此原則。

經由遠端存取的 Challenge-Handshake Authentication Protocol (CHAP) 或 IIS 內的 IAS 與 Digest Authentication 都要求遵循此原則。

如何防止使用者非必要性地變更密碼

除了以上的密碼原則外，有些組織要求集中化地控制所有的使用者。本節將說明如何防止使用者變更其密碼，除非他們被系統要求去進行變更。

使用者密碼的集中化控制對於設計巧妙的 Windows Server 2003 安全性機制而言，是相當重要的基礎。您可使用群組原則來設定最小和最大的密碼期限，如同先前所討論的。不過請記住，當您要求使用者時常變更密碼時，他們將可能規避您環境的密碼記錄設定。而要求過長的密碼也可能因為使用者忘記密碼，而產生更多的支援服務電話數。

使用者可在最小和最大的密碼期限之間變更其密碼。不過，高安全性的環境設計會要求使用者在作業系統設定後的第 42 天後提示他們變更時才變更密碼，如同 Maximum password age 設定值所設定的。為防止使用者變更其密碼 (除了被要求時)，您可在按下 CTRL+ALT+DELETE 所顯示的 Windows Security 對話方塊中停用 Change Password 選項。

您可透過群組原則，將此組態導入至整個網域內，或透過編輯登錄，將它導入到一個或多個特定的使用者上。如需此組態的詳細指示，請參閱 Microsoft 知識庫文件 324744，"How To: Prevent Users from Changing a Password Except When Required in Windows Server 2003"，網址為 <http://support.microsoft.com/default.aspx?scid=324744>。

帳戶鎖定機制

帳戶鎖定機制是一個 Windows Server 2003 安全性功能，它可在指定期間內發生特定次數的失敗登入記錄後，鎖定使用者帳戶。可容許的嘗試個數和期間取決於安全性原則鎖定設定值所設定的數值。使用者在帳戶鎖定後，並不能登入至鎖定的帳戶。Windows Server 2003 會追蹤登入嘗試次數，而伺服器軟體也可設定成 - 在經過預定個數的失敗登入之後，即停用該帳戶，以回應這類潛在的攻擊。

當管理員在 Windows Server 2003 內設定帳戶鎖定機制時，他可設定最大嘗試次數和期間變數。不過，若「Reset account lockout counter after」的設定值大於「Account lockout duration」設定值，Windows Server 2003 會自動將「Account lockout duration」的數值調成「Reset account lockout counter after」設定值。此外，若「Account lockout duration」的數值低於「Reset account lockout counter after」的數值，Windows Server 2003 會自動將「Reset account lockout counter after」的數值調成「Account lockout duration」設定值。因此，若「Account lockout duration」已定義，「Reset account lockout counter after」必須小於或等於「Account lockout duration」。

Windows Server 2003 如此做是為了避免安全性原則內的設定值發生衝突。若管理員將「Reset account lockout counter after」的設定值設成大於「Account lockout duration」設定值，那麼「Account lockout duration」設定值在套用時將會先過期，導致使用者可登入回網路中。不過，「Reset account lockout counter」設定值將會持續地倒數。由於此緣故，帳戶鎖定臨界值將會維持在最高的三次無效嘗試，並且使用者將無法登入。

為避免此狀況，Windows Server 2003 會自動將「Reset account lockout counter after」設定值重設成「Account lockout duration」設定值。這些安全性原則的設定值有助於防止駭客臆測使用者密碼，並減少成功地攻擊您網路環境的可能性。底下章節的數值可設定於下列位置的網域群組原則內：

Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy

Account Lockout Duration

表 2.9：設定值

網域成員預設值	舊版用戶端	企業用戶端	高安全性
未定義	30 分鐘	30 分鐘	15 分鐘

「Account lockout duration」設定值決定了要經過多少時間，帳戶方能解除鎖定，並讓使用者再次嘗試登入。此設定將會指定鎖定之帳戶無法使用的分鐘數來達到此目的。將「Account lockout duration」設定值設成 0，可讓帳戶維持鎖定，直到管理員解除其鎖定。此設定的 Windows Server 2003 預設值為「Not Defined (未定義)」。

雖然將此設定值設成絕不自動解除鎖定似乎是個不錯的點子，但如此做可能會增加您企業組織服務台接到的電話數——會接到一堆要求解除被錯誤鎖定的帳戶。將舊版和企業用戶端環境的設定值設成 30 分鐘，而高安全性層級設成 15 分鐘，將可減少拒絕服務 (Denial of Service，簡寫為 DoS) 攻擊所造成的額外作業負荷量。在 DoS 攻擊中，駭客會針對組織內的所有使用者惡意執行許多失敗的登入嘗試，以鎖定其帳戶。此設定值可會讓被鎖定的使用者有機會在 30 分鐘內再次登入，此時間是他們在尋求服務台協助前所能忍受的時間。

此手冊建議您在高安全性環境中將此數值設成 15 分鐘。

Account lockout threshold

表 2.10：設定值

網域成員預設值	舊版用戶端	企業用戶端	高安全性
0 個無效登入嘗試	50 個無效登入嘗試	50 個無效登入嘗試	10 個無效登入嘗試

Account lockout threshold 設定值決定了使用者在帳戶鎖定之前可嘗試登入幾次。

即使是經過授權的使用者，仍可能由於不正確地輸入密碼，或在一台電腦上變更密碼、同時又登入至另一台電腦，而讓自己鎖在帳戶之外。密碼不正確的電腦可能持續地嘗試驗證使用者，但由於它用來驗證的密碼是錯誤的，因此導致使用者帳戶最後被鎖定。為避免將授權的使用者的帳戶被鎖住，請將帳戶鎖定的上限值設成較大的數值。

因為不管此設定值有設定或沒設定，都可能漏洞，此處將替這一種可能性定義不同的對策。您的企業組織可根據您是否想要降低這些威脅和風險，來權衡這兩種選擇。

- 為避免帳戶鎖定，請將「Account lockout threshold」設定值設成「0」。將「Account Lockout Threshold」設定值設成「0」有助於減少打進服務台的電話數，因為使用者不會意外地將自己鎖到帳戶之外，它也可防止 DoS 攻擊刻意地鎖定您組織內的帳戶。但由於它無法防止暴力式攻擊，您只能在下列兩項準則符合時，方能選擇此設定：
- 密碼原則強力要求所有的使用者擁有由八個或更多字元組成的複雜密碼。
- 當系統環境內發生一系列的帳戶鎖定事件時，系統擁有一個健全的機制來提醒管理員。例如，稽核解決方案應該要監視安全性事件 539：「登入失敗。帳戶在企圖登入時被鎖住」。此事件意味著帳戶在登入嘗試臨界值設定時已鎖定。不過，事件 539 只會顯示帳戶鎖定，而無法顯示失敗的密碼嘗試。因此，您的管理員也應監視一系列的不良密碼嘗試。
- 若無法符合上述條件，第二個選擇是將「Account lockout threshold」設定值設成夠大的數值，以便讓使用者即便是意外地打錯幾次密碼，也不會將自己鎖在帳戶之外，同時又可在發生暴力式密碼攻擊時，將帳戶鎖住。在此狀況中，將無效的登入嘗試設成較大的數值，例如 50，可確保足夠的安全性與可接受性。此設定值可防止意外的帳戶鎖定，並減少服務台電話，但並無法防止 DoS 攻擊，如上所述。

本手冊建議您在高安全性環境中將此數值設成 10 個無效的登入嘗試。

Reset account lockout counter after

表 2.11：設定值

網域成員預設值	舊版用戶端	企業用戶端	高安全性
未定義	30 分鐘	30 分鐘	15 分鐘

「Reset account lockout counter after」設定值決定要經過多少時間，「Account lockout threshold」才會重設成「0」，並讓帳戶解除鎖定。若您定義了「Account lockout threshold」，那麼此重設時間必須小於或等於「Account lockout duration」設定值。

若您配合本手冊所設定的其他數值，即將此設定值保留其預設值，或將此數值設成過長的期間，則您的環境將很容易遭受帳戶鎖定的 DoS 攻擊。若重設帳戶鎖定並沒有任何原則，則系統管理員可能需要手動地去解除所有的帳戶鎖定。反過來說，如果將此設定值設成合理的時間，使用者可能會被鎖定一段時間，一直到所有的帳戶都自動解除鎖定。建議將其設定為30分鐘，這是在使用者能夠容忍不尋求服務台協助的時間範圍內。若您根據我們建議的方式變更了其他設定值，但將此設定保留為預設值，則您將可能遭受帳戶鎖定的 DoS 攻擊。縮短設定的時間，可減少拒絕服務 (DoS) 攻擊期間所額外增加的作業負荷量。在 DoS 攻擊中，駭客會惡意地針對組織中的所有使用者執行大量的失敗登入嘗試，來使其帳戶被系統鎖定。

本手冊建議您在高安全性環境中將此設定值設成 15 分鐘。

Kerberos 原則

Kerberos 原則用於網域使用者帳戶中。這些原則決定了 Kerberos 5 版通訊協定的相關設定，例如票證存留期間和強制使用。Kerberos 原則並不存在於本機電腦原則內。減少 Kerberos 票證的存留期可減少駭客竊取密碼、然後假扮合法使用者帳戶的風險。不過，維持這些原則將會增加授權的額外負荷。在大多數的環境中，這些原則的預設值都不應變更。Kerberos 設定包含於預設網域原則內，並強制使用於該處，因此本手冊並未將它們包含於本手冊附上的安全性範本中。

本手冊並未替預設的 Kerberos 原則提供任何變更。如需這些設定的進一步細節，請參閱所附的手冊《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》。

安全性選項

帳戶原則必須定義於預設網域原則(Default Domain Policy)內，並由組成該網域的網域控制器所強制使用。網域控制器每次都從預設網域原則(Default Domain Policy)GPO 中取得帳戶原則，即使有不同的帳戶原則套用至包含該網域控制器的 OU，也是如此。

安全性選項內有兩個原則，其運作方式類似於帳戶原則，且在網域層級中必須要考慮到。您可在下列位置的下列表格中設定網域群組原則的值：

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Microsoft 網路伺服器:當登入時間過期，則將用戶端斷線

表 2.12：設定值

網域成員預設值	舊版用戶端	企業用戶端	高安全性
未定義	啟用	啟用	啟用

Microsoft 網路伺服器:當登入時間過期，則將用戶端斷線，安全性設定值會決定當使用者在其使用者帳戶有效登入時數之外連結至本機電腦時，是否該切斷其連接。此設定將影響伺服器訊息區塊 (Server Message Block，簡寫為 SMB) 元件。若此原則被啟用，則當用戶端的登入時數過期時，此原則會使得包含 SMB 服務的用戶端工作階段強迫切斷連接。若此原則為停用，當用戶端的登入小時過期之後，已建立的用戶端工作階段仍可繼續進行。在啟用此設定時，您也應啟用「網路安全性:當登入時數到其實，強制登出。」

若您的企業組織已替使用者設定了登入小時，那啓用此原則才有意義，否則原本不能在登入小時之外存取網路資源的使用者，事實上卻可透過在系統容許小時內建立的工作階段，持續使用這些資源。

若您的企業組織並未使用登入小時，啓用此設定將沒有任何影響。若使用了登入小時，那麼當登入小時過期時，則現有的使用者工作階段將被強迫中斷。

網路存取:允許匿名 SID/NAME 轉換

表 2.13：設定值

網域成員預設值	舊版用戶端	企業用戶端	高安全性
未定義	停用	停用	停用

網路存取:允許匿名SID/NAME轉換設定值決定了匿名的使用者是否可要求另一個使用者的 SID。

若此原則在某個網域控制器上啟用，則知道某個管理員 SID 屬性的使用者便可聯絡及啟用此原則的電腦，並使用 SID 來取得管理員的名稱。接著此人就可使用該帳戶名稱發動密碼臆測攻擊。在成員電腦上，其預設值為停用；因此它對它們並沒有任何影響。不過，網域控制器的預設值為啟用。停用此設定可能導致舊版系統無法與以 Windows Server 2003 為基礎的網域進行通訊，例如：

- 以 Windows NT 4.0 為基礎的 Remote Access Service 伺服器。
- 當 IIS 上的 Web 應用程式設成允許基本驗證，同時又停用匿名存取，內建的 Guest 使用者帳戶將無法存取 Web 應用程式。此外，若您將內建的 Guest 使用者帳戶重新命名為其他名稱，新的名稱將無法用來存取 Web 應用程式。
- Remote Access Service 伺服器執行於 Windows NT 3.x 網域或 Windows NT 4.0 網域上的 Windows 2000 電腦中。

網路安全性:當登入時數到其實，強制登出

表 2.14：設定值

網域成員預設值	舊版用戶端	企業用戶端	高安全性
停用	啟用	啟用	啟用

網路安全性:當登入時數到其實，強制登出設定值決定的是否要將並非在使用者帳戶的有效登入時間內連至本地電腦的使用者中斷連接。此設定值將會影響 SMB 元件。

若啟用此原則，當用戶端登入小時過期後，系統會強迫中斷包含 SMB 伺服器的用戶端工作階段，並且使用者需等到其下個排定的存取時間，方能再登入系統。若停用此原則，當用戶端的登入小時過期之後，已建立的用戶端工作階段仍可維持。若要影響網域帳戶，此設定必須在預設網域原則之定義。

摘要

在檢查樹系、網域和組織單位 (OU) 設計以保護環境安全時，有許多設計上的考量。

研究及記錄企業組織特定自發性以及隔離需求是相當重要的。政治自發性、作業隔離、合法或規定的隔離都是設計複雜樹系所考慮的重要理由。瞭解如何控制服務系統管理員也相當重要。惡意的服務系統管理員可能對組織帶來極大的風險。在較低的層級中，惡意的網域管理員可存取樹系中任何網域的資料。雖然變更組織內的樹系或網域設計並不是件簡單的事，為防範企業內可能產生的安全性風險，這仍是必要的。根據服務系統管理員和資料系統管理員的需求，規劃組織內的 OU 部署也非常重要。本章詳細地探討了建立 OU 模型的細節，以使用 GPO 來持續管理企業中不同的伺服器角色。

最後，本章指出了檢查組織內所有網域層級設定的重要性。每個網域只能設定一組密碼、帳戶鎖定 and Kerberos 5 版的驗證通訊協定原則。其他的密碼和帳戶鎖定設定只會影響到成員伺服器上的本機帳戶。請試圖設定設定值來將其套用至網域內所有成員伺服器的組態，並確保這些設定能提供您的企業組織足夠的安全性等級。

詳細資訊

底下的資訊來源列出了在本產品發行之際，與建立網域基礎架構和 Windows Server 2003 密切相關的最新主題。

如需 Windows 2000、Windows XP 和 Windows Server 2003 帳戶和本機原則的詳細資訊，請參閱：
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsnetserver/proddocs/server/sag_sceacctpols.asp。

如需微軟安全性和隱私權的詳細資訊，請參閱：<http://www.microsoft.com/security>。

如需十個安全性不變法則的相關資訊，請參閱：
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/10imlaws.asp>。

如需在 Active Directory 中委派管理的設計考量相關資訊，請參閱：<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/ad/windows2000/plan/addeladm.asp>。

如需設定時間伺服器的相關資訊，請參閱：Microsoft 知識庫文件 “How to Configure an Authoritative Time Server in Windows 2000”，網址為：<http://support.microsoft.com/default.aspx?scid=216734>。

如需網路存取和允許 SID/NAME 轉譯的相關資訊，請參閱：<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/623.asp>。

如需網路安全性和在登入小時過期時強迫登出的相關資訊，請參閱：<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/566.asp>。

Guest 帳戶不能用於匿名存取停用時，<http://support.microsoft.com/default.aspx?scid=kb;en-us;251171>。

3. 建立成員伺服器基礎

概觀

本章說明了管理所有執行 Microsoft® Windows Server 2003 的伺服器所需的基本安全性範例的設定需求。本章也提供在三個企業環境中進行系統管理的指引，幫助您安裝並設定具安全性的 Windows Server 2003 系統。本章的設定需求已成為所有其他的補強程序之基礎 (該補強程序也為本手冊後面各章所討論的特定伺服器角色所套用)。

本章所建議的設定，為企業環境中的商業應用程式伺服器建構一個穩固的基礎。不過，在將其導入生產環境之前，您必須完整地測試這些安全性設定與您企業組織中商業應用程式間的共存性。

本章所提出的設定建議，可應用在大部份的企業中，同時也可以部署在執行 Windows Server 2003 現存或新的系統上。Windows Server 2003 預設的安全性設定都已經過研究、重複檢視及測試。如需所有預設設定的相關資訊，以及本章所討論各設定的詳細解釋的資訊，請參閱所附手冊《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》，網址為<http://go.microsoft.com/fwlink/?LinkId=15159>。但，下述大部份設定建議的安全性都高於預設設定的安全性。

在本章中所有關於企業環境中 Windows Server 2003 系統的基礎安全性設定的討論，都與下面定義的三個系統環境有關。這些環境是：

- 舊版用戶端 (Legacy Client) – 提供足夠安全性，但將不會對混合狀態的環境造成限制。「舊版用戶端」等級是針對舊版用戶端的環境。這環境是本手冊所定義的最低層的「鎖定」等級。爲了要有更安全的環境，您的企業組織也可以選擇搬移到下一個鎖定等級，也就是「企業用戶端」等級，如果他們沒有保護舊版用戶端的必要，則可以此等級開始。這種商業環境包括了 Microsoft Windows® 98、Microsoft Windows NT® version 4.0 Workstation、Window 2000 Professional，以及 Windows XP Professional 工作站。但此環境只包含 Windows 2000 或以上的網域控制站。在此系統環境中沒有 Windows NT 4.0 網域控制站，但存在 Windows NT 成員伺服器。
- 企業用戶端 (Enterprise Client) – 提供新的系統環境所需的高度安全性。這種商業環境包括執行 Windows 2000 Professional 和 Windows XP Professional 的用戶端。由舊版環境搬移到企業環境絕大部份的工作都牽涉到舊版用戶端的升級，例如，Windows 98 和 Windows NT 4.0 Workstation 升級到 Windows 2000 或 Windows XP。此系統環境中所有的網域控制站都是 Windows 2000 Server 或以上。而系統環境中的成員伺服器則是 Windows 2000 Server 或以上。
- 高安全性 (High Security) – 提供較前一項企業用戶端等級爲強大的安全性標準。由企業用戶端環境遷移到高安全性環境，用戶端和伺服器二者都必須遵守嚴格的安全性原則。這環境包含了用戶端執行 Windows 2000 Professional、Windows XP Professional，而網域控制站執行 Windows 2000 Server 或以上等級。在高安全性環境中，對安全性的需求極高，甚至會考慮犧牲重要的功能性和管理性來達到最高等級的安全性。這環境中的成員伺服器是 Windows 2000 Server 或以上。

下圖顯示這三個等級的安全性，和每個等級支援的用戶端。

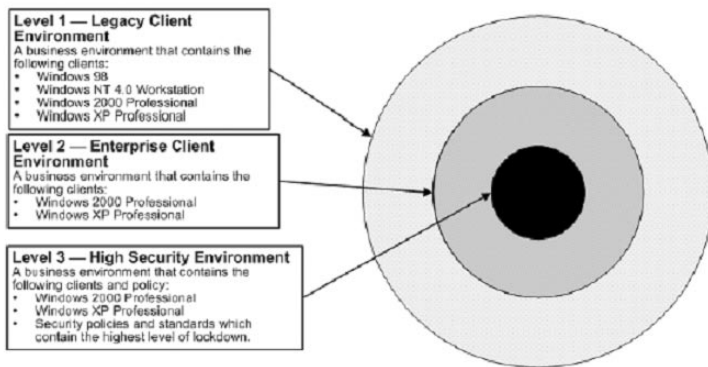


圖 3.1

現存與計畫中的鎖定等級

企業組織若想要以階段性漸進的方式來保護他們系統環境，可從「舊版用戶端」環境等級開始，待他們的應用程式和用戶端電腦升級，並經過較嚴謹的安全性設定測試後，再逐漸搬移到較高安全性等級。

下圖顯示了安全性範例 .inf 檔案如何作為企業用戶端 — 「成員伺服器基礎原則」 (Member Server Baseline Policy, 簡稱為 MSBP) 的基礎。下圖也顯示連結這原則，並套用在組織中所有伺服器可行辦法。Windows Server 2003 在出廠時的預設值便已經設成安全的狀態。在很多例子中，本章說明了設定方法，而非預設值，而在本手冊中所定義的三個系統環境，則強制使用特定的預設值。如需所有預設值的相關資訊，請參閱所附的手冊，《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》，網址為：<http://go.microsoft.com/fwlink/?LinkId=15159>。

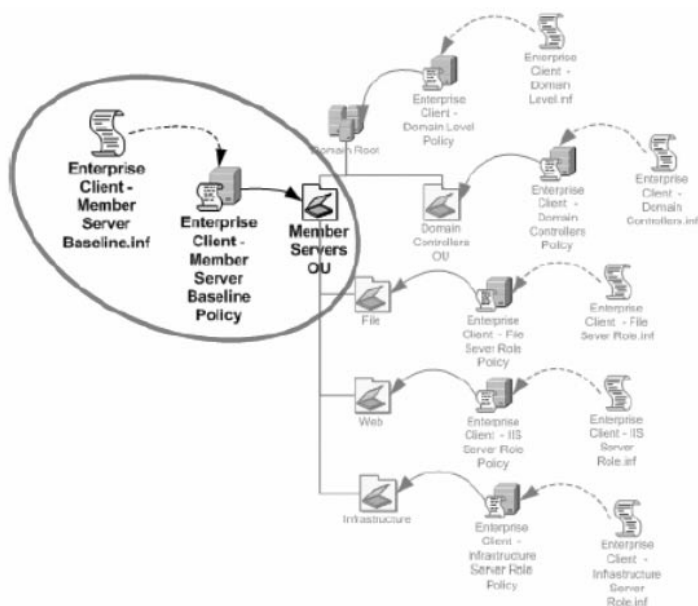


圖 3.2

安全性範例 Enterprise Client-Member Server Baseline.inf 匯入到 MSBP，然後 MSBP 連結到成員伺服器組織單位 (OU)

特定伺服器角色的補強程序是在本手冊的其他章節做定義。本手冊中主要的伺服器角色包括了：

- 網域控制站，它包括了 DNS (Domain Name System，網域名稱系統) 服務。
- 基礎架構伺服器角色，包括了：
 - WINS (Windows Internet Name Service，即 Windows 網際網路名稱服務)。
 - DHCP (Dynamic Host Configuration Protocol，動態主機設定通訊協定)。
- 檔案。
- 列印。
- IIS (Internet Information Services，網際網路資訊服務)。
- Microsoft IAS (Internet Authentication Server，網際網路驗證伺服器)。
- CA (Certificate Services servers，憑證服務伺服器)。
- 防禦主機 (Bastion Hosts)。

下面許多出現在企業用戶端(Enterpirce Client) 遵循MSBP的設定，也同樣適用本手冊所定義的三個系統環境中的伺服器角色。這些安全性範例是針對每一個獨特環境的安全性需求所設計的。下表顯示基礎安全性範例和這三個系統環境間的關係。如果您有需要特別區別是舊版用戶端、企業用戶端亦或是高安全性等級，與文中建議的基礎原則相關的安全性範例包含了等級識別，可讓您分辨其正確的範例。例如，Enterprise Client-Member Server Baseline.inf 檔案，是為「企業用戶端」環境所建議的安全性範例。

表 3.1：三個系統環境的基礎安全性範例

舊版用戶端	企業用戶端	高安全性
Legacy Client -	Enterprise Client -	High Security -
Member Server Baseline.inf	Member Server Baseline.inf	Member Server Baseline.inf

在所有環境 Member Server Baseline.inf 安全性範例中共同的安全性設定，將在本節接下來的「Windows Server 2003 基礎原則」部份中作描述。這些基礎安全性範例，也是第四章「補強網域控制站」所定義的網域控制站安全性範例的起點。

Enterprise Client-Domain Controllers Role.inf 範例提供「網域控制站群組原則」(Domain Controllers Group Policy) 的「群組原則物件」(GPO)基礎，且在這三個系統環境中，都連結到網域控制站的組織單位(OU)。在第二章「設定網域基礎架構」，我們提供您詳細步驟來協助您建立 OU 和群組原則，並將適當的安全性範例匯入每個 GPO 中。

注意：有些補強程序不能自動使用群組原則，他們將在本章「其他成員伺服器補強程序」這部份做描述。

Windows Server 2003 基礎原則

在成員伺服器 OU 等級中的設定定義了網域中所有成員伺服器的共通設定。其是透過建立一個連結到成員伺服器 OU 的 GPO 來完成的，即所謂的基礎原則。GPO 可將在每一台伺服器中設定特定安全性設定值的作業自動化。下面這些設定，是依據「安全性設定編輯器」(Security Configuration Editor，簡稱爲 SCE) 這嵌入式管理單元的使用者介面 (UI) 中所呈現的方式去描述。

稽核原則

系統管理員應該安裝一個稽核原則。這稽核原則會決定要報告給網路系統管理員的安全性事件為何，使得使用者或系統所發生的活動是在特定事件種類中的，便能夠記錄下來。系統管理員可以監視與安全性有關的活動，例如誰存取了某一物件、使用者是否登入或登出電腦，或者稽核原則設定的做了變更。

在導入稽核原則之前，必須先決定在公司環境中，哪些事件種類需要被稽核。系統管理員所選定的事件種類之稽核設定便定義了公司的稽核原則。藉著定義特定事件種類的稽核設定，系統管理員可以建立一個適合企業組織安全性需求的稽核原則。

如果設定成沒有稽核，就很難或根本不可能判定意外事件中是否發生了危急安全性的事件。然而，如果稽核設定設了太多授權活動所產生的事件，那麼事件記錄檔便會存放一堆無用的資料。因此，接下來我們的建議主要目的是協助您作出做適當的決定，來看監視哪些事件才能夠使得收集的資料都是有意義的。

下表包括了適用此手冊所定義三個系統環境的稽核原則建議。您也許會發現，這三種環境的大部份設定值都非常類似。

底下這些值可以在 Windows Server 2003 「網域群組原則」下的下述設定：

Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy

如需本節所定的設定摘要，請參閱 Windows Server 2003 Security Guide Settings Microsoft Excel 工作簿。如需預設設定的相關資訊，及此節所討論的每個設定的詳細說明資訊，請參閱所附手冊 《Threats and Countermeasures：Security Settings in Windows Server 2003 and Windows XP》，網址為：<http://go.microsoft.com/fwlink/?LinkId=15159>。

帳戶登入事件

表 3.2：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
成功	成功 失敗	成功 失敗	成功 失敗

帳戶登入事件(Account Logon Event)的設定決定是否要稽核每次使用者登入或登出另一台經確認帳戶的電腦。驗證網域控制站的網域使用者帳戶會產生一個帳戶登入事件。此事件會記錄在網域控制站的安全性記錄檔中。驗證本機電腦的就地使用者也會產生一個登入事件。此事件是記錄在本機的安全性記錄檔中。此外，並不會記錄帳戶登出事件。

下表包括了一些會記錄於「安全性事件記錄檔」(Security Event Log) 的重要安全性事件的設定。

表 3.3：帳戶登入事件

事件 ID	事件描述
672	驗證服務 (AS) 票證已成功地發出並確認。
673	票證授與服務 (ticket granting service, 簡寫為 TGS) 的票證已授與。TGS 是 Kerberos version 5 票證授與服務所發行的票證。TGS 允許使用者向網域的特定服務申請驗證。
674	安全性本體重新更新 AS 票證或 TGS 票證。
675	驗證之前失敗。此事件是金鑰發佈中心 (Key Distribution Center, 簡稱為 KDC) 在使用者輸入不正確的密碼時所產生。
676	驗證票證的要求失敗。此事件在 Windows XP Professional 或 Windows 伺服器家族的成員中不會產生。
677	TGS 票證未被授與。此事件在 Windows XP Professional 或 Windows 伺服器家族的成員中不會產生。
678	帳戶成功地對應到網域帳戶。
681	登入失敗。企圖登入網域帳戶。此事件在 Windows XP Professional 或 Windows 伺服器家族的成員中不會產生。
682	使用者重新連線到已停止連線的終端機伺服器工作期間。
683	使用者沒有登出就從終端機伺服器工作期間停止連線。

上表的事件 ID (識別碼), 在您所建立用以監視任何軟體套件的自訂警告, 例如 Microsoft Operations Manager (MOM) 時可能很有用。

稽核帳戶管理

表 3.4：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
沒有稽核	成功 失敗	成功 失敗	成功 失敗

稽核帳戶管理(Audit Account Management)的設定可決定是否要稽核電腦上的每個帳戶管理事件。帳戶管理事件的例子包括：

- 使用者帳戶或群組的建立, 變更, 或刪除。
- 使用者帳戶重新命名, 停用, 或啓用。
- 密碼設定或變更。

企業組織需要知道誰已經建立、修改, 或刪除網域及本機帳戶。未經授權的變更也可能意味某個系統管理員沒有遵循公司的原則, 而作了錯誤性變更, 或來自故意的攻擊。

例如, 帳戶管理失敗事件通常代表了一個較低層級的系統管理員, 或是一個侵入較低層級系統管理員帳戶的駭客, 也許正企圖提高他的權限。您可以透過記錄來看駭客變更或建立了那些帳戶。

基於此理由，在三個系統環境中我們所提供的設定對策都是把它設定成同時包括「Success (成功)」和「Failure (失敗)」二種。下表包括了一些會記錄於安全性事件記錄檔的重要安全性事件的設定。

表 3.5：帳戶管理事件

事件 ID	事件描述
624	使用者帳戶被建立。
627	使用者密碼被變更。
628	使用者密碼被設定。
630	使用者帳戶被刪除。
631	通用群組 (global group) 被建立。
632	成員加入通用群組。
633	成員由通用群組移除。
634	通用群組被刪除。
635	新的區域群組 (local group) 被建立。
636	成員被加入區域群組。
637	成員由區域群組移除。
638	區域群組被刪除。
639	區域群組帳戶被變更。
641	通用群組帳戶被變更。
642	使用者帳戶被變更。
643	網域原則被修改。
644	使用者帳戶被自動鎖定。
645	電腦帳戶被建立。
646	電腦帳戶被變更。
647	電腦帳戶被刪除。
648	安全性停用 (security disabled) 的區域安全性群組被建立。 注意：正式名稱爲 SECURITY_DISABLED，其意義是這群組在存取檢查時，不能用來授與權限。
649	安全性停用的區域安全性群組被變更。
650	成員被加入安全性停用的區域安全性群組。
651	成員由安全性停用的區域安全性群組移除。

652	安全性停用的區域群組被刪除。
653	安全性停用的通用群組被建立。
654	安全性停用的通用群組被變更。
655	成員被加入安全性停用的通用群組。
656	成員由安全性停用的通用群組移除。
657	安全性停用的通用群組被刪除。
658	安全性啓用的萬用群組 (universal group) 被建立。
659	安全性啓用的萬用群組被變更。
660	成員加入安全性啓用的萬用群組。
661	成員由安全性啓用的萬用群組移除。
662	安全性啓用的萬用群組被刪除。
663	安全性停用的萬用群組被建立。
664	安全性停用的萬用群組被變更。
665	成員加入安全性停用的萬用群組。
666	成員由安全性停用的萬用群組移除。
667	安全性停用的萬用群組被刪除。
668	群組類別被變更。
684	系統管理群組成員的安全性描述項被設定。 注意：網域控制站每隔 60 分鐘，一個幕後的執行緒就會搜尋所有系統管理群組 (例如網域、企業，及架構管理員) 的成員，並套用一固定的安全性描述項於其上。此事件會被記錄。
685	帳戶名稱被變更。

上表的事件 ID，在您建立自訂的警告以監視任何軟體套件，例如 MOM 時可能很有用。多數操作管理軟體都能以指令碼 (scripts) 自訂，以便能夠以上表的事件 ID 為基礎來捕捉或記錄事件。

稽核目錄服務存取

表 3.6：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
沒有稽核	成功 失敗	成功 失敗	成功 失敗

稽核目錄服務存取(Audit directory service access) 的設定可決定是否稽核使用者存取自己特定的「系統存取控制清單」(system access control list，簡稱為 SACL) 的 Microsoft Active Directory? 目錄服務物件的事件。將「稽核目錄服務存取(Audit directory service access)」設定為「No Auditing (沒有稽核)」會使得在安全性意外事件中，很難或根本不能判定哪些Active Directory 物件可能被攻擊。如果這個設定的值不是設成「Success (成功)」和「Failure (失敗)」，那麼在安全性意外事件發生後，將不會有明顯的稽核記錄可供分析了。

將「稽核目錄服務存取(Audit directory service access)」設定為「Success (成功)」，則每次使用者成功地以指定的 SACL 存取 Active Directory 物件時，便會產生一個稽核項目。將此設定設為「Failure (失敗)」，則每次使用者企圖以指定的 SACL 存取 Active Directory 物件失敗時，便會產生一個稽核項目。

表 3.7：目錄服務存取事件

事件 ID	事件描述
566	一般性的物件動作發生。

稽核登入事件

表 3.8：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
成功	成功 失敗	成功 失敗	成功 失敗

稽核登入事件(Audit Logon Event) 的設定可決定每次使用者登入登出電腦時是否作稽核記錄。公司可以透過稽核登入事件(Audit Logon Event) 設定所產生的記錄，來在網域控制站上監視網域帳戶活動，並在本機電腦上監視本機帳戶的活動。

將「稽核登入事件(Audit Logon Event)」設定成「No auditing (沒有稽核)」，將會很難或根本無法判定那個使用者已登入，或企圖登入企業中的電腦。在網域成員上，把「稽核登入事件(Audit Logon Event)」設定啟用為「Success (成功)」，則每次有人登入系統，不論帳戶位於系統何處，都會產生一個事件。如果使用者以本機帳戶登入，且「Audit account logon events (稽核帳戶登入事件)」設定是「Enabled (啟用)」的狀態，則使用者登入將會產生兩個事件。

在本手冊所定義三個安全性環境中，如果這個設定的值不是設成「Success (成功)」和「Failure (失敗)」，那麼在安全性意外事件發生後，將會沒有明顯的稽核記錄可供分析了。

表 3.9：稽核登入事件

事件 ID	稽核登入事件
528	使用者成功地登入電腦。
529	登入失敗。不知名的使用者企圖登入，或知名的使用者密碼錯誤。
530	登入失敗。允許時間外企圖登入。
531	登入失敗。企圖以已停用帳戶登入。
532	登入失敗。企圖以已過期帳戶登入。
533	登入失敗。不被允許登入特定電腦的使用者企圖登入。
534	登入失敗。使用者企圖以不被允許的密碼類型登入。
535	登入失敗。特定帳戶的密碼已過期。
536	登入失敗。網路登入 (Net Logon) 服務不在作用中。
537	登入失敗。由於其他原因，企圖登入失敗。 注意：在一些情況中，登入失敗的原因不明。
538	使用者完成了登出過程。
539	登入失敗。企圖登入時，帳戶被鎖定。
540	使用者成功地登入網路。
541	在本機電腦與所列對等端個體 (peer identity) 之間 (建立安全性連結) 的主模式「網際網路金鑰交換」(IKE) 驗證已完成，或是快速模式已建立資料通道。
542	資料通道已終止。
543	主模式已終止。 注意：可能導致的原因為，安全性連結的時間限制已到 (預設值是八小時)，原則變更，或對等端終止 (peer termination)。
544	主模式驗證失敗，因為對等端未提供正確的憑證，或是簽章未經確認。

(接上頁)

545	主模式驗證失敗，因為 Kerberos 失敗或密碼不正確。
546	IKE 安全性連結建立失敗，因為對等端傳送不正確的申請。收到含有不正確資料的封包。
547	進行 IKE 信號交換 (handshake) 時發生失敗。
548	登入失敗。由信任的網域來的安全性識別項 (SID)，與用戶端帳戶網域的 SID 不相符。
549	登入失敗。所有不被信任的名稱空間對應的 SID，在跨樹系的驗證中，全部被篩選掉。
550	通知訊息表示可能有拒絕服務 (DoS) 攻擊。
551	使用者起始登出過程。
552	使用者成功地使用明顯憑證登入電腦，但同時又已經以另一個使用者身份登入。
682	使用者重新連線到已停止連線的終端機伺服器工作階段。
683	使用者停止終端機伺服器工作階段連線，卻沒有登出。 注意：此事件產生於使用者透過網路連線到終端機伺服器工作階段時。它會呈現在終端機伺服器。

稽核物件存取

表 3.10：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
沒有稽核	成功 失敗	成功 失敗	成功 失敗

此設定本身不會產生任何稽核事件。Audit object access (稽核物件存取) 的設定可決定是否稽核使用者存取擁有特定 SACL 物件的事件，例如，存取檔案、資料夾、登錄機碼、印表機等等。

SACL 是由存取控制項目 (ACE) 組成。每個 ACE 包含三項資訊：

- 被稽核的安全性主體 (使用者、電腦、或群組)。
- 被稽核的特定存取類型，稱作「存取遮罩」(access mask)。
- 表示是否要稽核失敗存取事件、成功存取事件、或是兩者都要的旗標。

將此設定設為「Success (成功)」，則每次使用者成功地以特定的 SACL 存取物件時，便會產生一個稽核項目。將此設定設為「Failure (失敗)」，則每次使用者以特定的 SACL 存取物件失敗時，便會產生一個稽核項目。公司應在設定 SACL 時，只定義那些他們想啓用的動作。例如，您也許想透過執行檔來啓用「Write and Append Data auditing (寫入與增添資料稽核)」的設定，以追蹤登入者對那些檔案進行取代或變更，這是電腦病毒和特洛伊木馬病毒最長導致的結果。同樣的，您也許想針對敏感的文件，追蹤變更，甚至讀取的動作。

因此，我們建議您將對手冊所定義三個系統環境都啟用設定的「Success (成功)」和「Failure (失敗)」兩個稽核值。

表 3.11：物件存取事件

事件 ID	事件描述
560	允許存取已經存在的物件。
562	物件的控制代碼已經關閉。
563	嘗試開啓某個物件，並企圖刪除它。 注意：當 FILE_DELETE_ON_CLOSE 旗標指定於 Createfile() 時，此 ID 將由檔案系統所使用。
564	受保護的物件被刪除。
565	允許存取已經存在的物件類型。
567	使用了與控制代碼相關的權限。 注意：控制代碼是以某些授與的權限 (讀取、寫入等等) 來建立。當控制代碼被使用時，最多會替每個使用的權限產生一個稽核。
568	嘗試替正被稽核的檔案建立一個硬連結。
569	Authorization Manager 內的資源管理員嘗試建立用戶端內容。
570	用戶端嘗試存取物件。 注意：嘗試在物件上執行的每項操作都會產生一個事件。
571	用戶端內容已被 Authorization Manager 應用程式所刪除。
572	Administrator Manager 已初始化應用程式。
772	Certificate Manager 拒絕暫止的認證要求。
773	認證服務收到再次送出的認證要求。
774	認證服務取消某個認證。
775	認證服務收到一個要求，要它發行認證取消清單 (CRL)。
776	認證服務已發行 CRL。
777	認證要求擴充功能已完成。
778	一個或多個認證要求屬性已變更。
779	認證服務收到一個關機要求。
780	認證服務備份已啓動。
781	認證服務備份已完成。
782	認證服務還原已啓動。

(接上頁)

783	認證服務還原已完成。
784	認證服務已啟動。
785	認證服務已停止。
786	認證服務的安全性權限已變更。
787	認證服務擷取出一個保存金鑰。
788	認證服務將認證匯入其資料庫內。
789	認證服務的稽核篩選器已變更。
790	認證服務收到一個認證要求。
791	認證服務核准一個認證要求，並發出一個認證。
792	認證服務拒絕一個認證要求。
793	認證服務將認證要求的狀態設成暫止。
794	認證服務的認證管理員設定已變更。
795	認證服務中的組態項目已變更。
796	認證服務的屬性已變更。
797	認證服務已保存某個金鑰。
798	認證服務已匯入與保存某個金鑰。
799	認證服務已發行認證授權 (CA) 認證給 Active Directory。
800	一列或多列已從認證資料庫中刪除。
801	角色分隔已啟用。

稽核原則變更

表 3.12：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
沒有稽核	成功	成功	成功

Audit policy change (稽核原則變更) 的設定會決定是否要稽核使用者權限設定原則、稽核原則或信任原則的每一項變更事件。這包括了變更稽核原則本身。

若將此設定設成「Success (成功)」，則每次使用者權限設定原則、稽核原則或信任原則變更成功時，都會產生一個稽核項目。若將此設定設成「Failure (失敗)」，則每次使用者權限設定原則、稽核原則或信任原則變更失敗時，都會產生一個稽核項目。

我們所建議的設定可讓您檢視駭客企圖提高任何帳戶權限的事件，例如，加入「Debug programs」權限或「Back up files and directories」權限。原則變更的稽核作業也包括稽核原則本身以及信任關係的變更。

注意：本手冊建議您將此設定設成「Success (成功)」即可，因為包含「Failure (失敗)」的設定值並不會提供有意義的存取資訊。目前，將此值設成「Failure (失敗)」並無法擷取到有意義的事件。

表 3.13：稽核原則變更事件

事件 ID	事件描述
608	使用者權限已指定。
609	使用者權限已移除。
610	與另一個網域的信任關係已建立。
611	與另一個網域的信任關係已移除。
612	稽核原則已變更。
613	Internet Protocol Security (IPSec) 原則代理程式已啟動。
614	IPSec 原則已停用。
615	IPSec 原則代理程式已變更。
616	IPSec 原則代理程式碰到一個潛在的嚴重失敗。
617	Kerberos 5 版的原則已變更。
618	Encrypted Data Recovery 原則已變更。
620	與另一個網域的信任關係已修改。
621	系統存取權限已授與某個帳戶。

(接上頁)

622	系統存取權限已從某個帳戶中移除。
623	稽核原則已根據每一使用者方式來設定。
625	稽核原則已根據每一使用者方式重新整理。
768	偵測到某個樹系中的一個命名空間項目和另一個樹系內的某個命名空間項目發生衝突 (Collision)。 注意：當某個樹系內的命名空間項目和另一個樹系內的命名空間項目互相重疊時，說明該命名空間的某個項目名稱可能會產生模稜兩可的狀況。此重疊也稱為衝突 (Collision)。並非所有的參數對於每個項目類型都有效。例如，像 DNS 稱、NetBIOS 名稱和 SID 等欄位就不適用於 'TopLevelName' 類型的項目。
769	受信任的樹系資訊已加入。 注意：此事件訊息的產生適當樹系信任資訊已更新，並加入一個或多個項目時。每個加入、刪除或修改的項目都會產生一個事件訊息。若在單次的樹系信任資訊更新時，加入、刪除或修改多個項目，所有產生的事件訊息都會指定一個唯一的識別碼，稱為作業 ID。這可讓您判斷多個產生的事件訊息是否為單一作業的結果。並非所有的參數對於每個項目類型都有效。例如，像 DNS 名稱、NetBIOS 名稱和 SID 等欄位就不適用於 'TopLevelName' 類型的項目。
770	受信任的樹系資訊已刪除。 注意：請參閱事件 769 的事件描述。
771	受信任的樹系資訊已修改。 注意：請參閱事件 769 的事件描述。
805	事件記錄服務可讀取某个工作階段的安全性記錄組態。

稽核權限的使用

表 3.14：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
沒有稽核	沒有稽核	失敗	成功 失敗

Audit privilege use (稽核權限使用) 的設定決定是否要稽核每個執行使用者權限的使用者執行個體。將此值設成「Success (成功)」，則可在每次使用者權限運用成功時產生一個稽核項目。將此值設成「Failure (失敗)」，則可在每次使用者權限運用失敗時產生一個稽核項目。

即使將「Audit privilege use (稽核權限使用)」設定設成「Success (成功)」或「Failure (失敗)」，稽核也不會在下列使用者權限執行時產生。這是因為稽核這些使用者權限會在安全性記錄檔中產生許多事件，進而降低電腦的效能。若要稽核下列排除在外的權限，您必須啓用群組原則內的稽核(Audit)：「Audit the use of Backup and Restore privilege(稽核備份及復原權限)」安全性選項：

- 略過往返檢查。
- 偵錯程式。
- 建立權杖 (Token) 物件。
- 取代處理序層級的權杖。
- 產生安全性稽核。
- 備份檔案和目錄。
- 復原檔案和目錄。

啓用權限稽核會產生大量的事件記錄。基於此理由，此手冊所定義的每個安全性環境對於這些設定都有不同的建議值。無法使用使用者權限是一般網路出問題的訊號，通常也代表了正有人嘗試利用安全性漏洞。除非有特殊的商業理由，否則公司不應將「Audit privilege use (稽核權限使用)」的設定值設成「Enable(啓用)」。

表 3.15：權限使用事件

事件 ID	事件描述
576	指定的權限已加到使用者的存取權限內。 注意：此事件產生於使用者登入時。
577	使用者嘗試執行授權的系統服務作業。
578	權限已在受保護物件的已開啓控制代碼上。

稽核流程追蹤

表 3.16：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
沒有稽核	沒有稽核	沒有稽核	沒有稽核

Audit process tracking (稽核處理序追蹤) 的設定值可決定是否要稽核詳細的事件追蹤資訊，例如程式啓動、處理序結束、控制代碼重複、間接物件存取。若將此設定設成「Success (成功)」，則每次成功地追蹤到處理序時，就會產生一個稽核項目。若將此設定設成「Failure (失敗)」，則每次無法追蹤到處理序時，就會產生一個稽核項目。

啓用「Audit process tracking (稽核處理序追蹤)」會產生大量事件，因此一般它都設成「(No Auditing)不稽核」。不過，這些設定值依舊帶來極大的好處，因為它提供了詳細的處理序啓動記錄，以及它們的啓用時間。

表 3.17：詳細的追蹤事件

事件 ID	事件描述
592	新的處理序已建立。
593	處理序已結束。
594	物件的控制代碼已重複。
595	物件的間接存取已取得。
596	資料保護主金鑰已備份。 注意：主金鑰是由 CryptProtectData 和 CryptUnprotectData 常式以及 Encrypting File System (EFS) 所使用。主金鑰將備份於每次新的金鑰建立時。(預設值為 90 天。)金鑰通常是由網域控制站所備份。
597	資料保護主金鑰已從復原伺服器中復原。
598	可稽核的資料已受到保護。
599	可稽核的資料已解除保護。
600	一個處理序被指定一個主要權限。
601	使用者嘗試安裝服務。
602	排程器工作已建立。

稽核系統事件

表 3.18：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
沒有稽核	成功	成功	成功

Audit system events (稽核系統事件) 的設定可決定是否要稽核使用者何時重新啓動電腦或關機的事件，或是何時發生會影響系統安全性或安全性記錄檔的事件。若將此設定設成「Success (成功)」，則當系統事件執行成功時，便會產生一個稽核項目。若將此設定設成「Failure (失敗)」，則當系統事件執行失敗時，便會產生一個稽核項目。

下表包含了這個類別中最有用的成功事件。

表 3.19：稽核系統事件的系統事件訊息

事件 ID	事件描述
512	Windows 正在啟動。
513	Windows 正在關機。
514	驗證封裝已由 Local Security Authority 所載入。
515	受信任的登入處理序已向 Local Security Authority (本機安全性授權) 註冊。
516	配置給安全性事件訊息佇列的內部資源已用盡，導致一些安全性事件訊息遺失。
517	稽核記錄檔已清除。
518	通知封裝已由 Security Accounts Manager 載入。
519	處理序正在使用無效的本地程序呼叫 (LPC) 連接埠，嘗試模擬一個用戶端，並回覆、讀取或寫入至用戶端位址空間。
520	系統時間已變更。 注意：此稽核通常會出現兩次。

使用者權利設定

User Rights Assignments (使用者權利設定) 可決定哪些使用者或群組在您組織的電腦上擁有登入的權利或權限。登入權利或權限將控制使用者在目標系統上所擁有的權限。它們將用來授與執行某些動作的權限 (例如從網路或本機登入) 以及管理員工作 (例如產生新的登入權杖)。

注意：在底下的章節中，User Rights Assignments “未定義” 意味著管理員仍擁有每個未定義權利的權限。本機管理員可自行變更，但是下次群組原則重新整理或重新套用時，任何網域型態的群組原則又會蓋過它們。

若要將 User Rights Assignments 設定在 Windows Server 2003 中，則可設定於「群組原則物件編輯器」中的下列位置：

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

預設的 User Rights Assignments 將隨著您企業中的伺服器類型而有差異。例如，User Rights Assignments 在 Windows Server 2003 的成員伺服器和網域控制站的內建群組間有下列的差異。成員伺服器和網域控制站間的類似內建群組並未記錄在底下的清單內。

成員伺服器

- Power Users
Power Users 擁有大多數的管理能力，不過也有一些限制。因此，Power Users 可執行已認證應用程式以外的舊版應用程式。
- HelpServicesGroup
這是「說明及支援中心」的群組。Support_388945a0 在預設狀態下為此群組的成員。
- TelnetClients
此群組的成員可存取系統上的 Telnet Server。

網域控制站

- Server Operators
此群組的成員可管理網域伺服器。
- Terminal Server License Services
此群組的成員可存取系統上的 Terminal Server License Servers。
- Windows Authorization Access Group
此群組的成員可存取使用者物件上的運算 tokenGroupsGlobalAndUniversal 屬性。

群組 Guests 和使用者帳戶 Guest 與 Support_388945a0 在不同的網域間擁有唯一的 SID。因此，在只包含特定目標群組的系統上，您可能需要修改此使用者權限設定的群組原則。此外，原則範本亦可個別做編輯，以便將適當的群組包含於 .inf 檔內。例如，網域控制站的群組原則應建立於測試環境中的網域控制站中。

注意：由於 Guests、Support_388945a0 和 Guest 間存在唯一 SID，一些強化設定並無法使用本手冊所包含的安全性範本來進行自動化作業；這些事項都會在本章後面的「額外的成員伺服器強化程序」小節中說明。

本節詳細說明在 MSBP 中，對於本手冊所定義三個系統環境所預定的使用者權限設定。如需本節所預定的設定摘要，請參閱 Windows Server 2003 Security Guide Settings Excel 工作簿。如需預設設定的相關資訊，及此節所討論的每個設定的詳細說明資訊，請參閱所附手冊《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》，網址為：<http://go.microsoft.com/fwlink/?LinkId=15159>。

從網路上存取本電腦

表 3.20：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員、備份操作員、Everyone、Power Users 和使用者	未定義	未定義	管理員、驗證過的使用者

Access this computer from the network (由網路存取本電腦) 這使用者權限，可決定哪些使用者和群組允許透過網路連接到此電腦。這項使用者權限是許多網路通訊協定所必需的，包括了以伺服器訊息區塊 (SMB) 為基礎的通訊協定、網路基本輸入輸出系統 (NetBIOS)、共同網際網路檔案系統 (CIFS)、Hypertext 傳輸通訊協定 (HTTP) 以及 Component Object Model Plus (COM+)。

雖然在 Windows Server 2003 中，授權給「Everyone (每個人)」安全性群組的權限將不再授與存取權給匿名使用者，但 guest 群組和帳戶仍可能透過「Everyone (每個人)」安全性群組獲得存取權。基於此理由，本手冊建議在高安全性的系統環境中，從「Access this computer from the network (由網路存取本電腦)」的使用者權限移除「Everyone (每個人)」的安全性群組，以進一步防護企圖以「Guest(訪客)」存取網域的攻擊。

成為作業系統的一部份

表 3.21：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
未定義	未定義	未定義	取消所有的安全性群組和帳戶

Act as part of the operating system (成為作業系統的一部份) 使用者權限可讓處理序假裝是任意使用者的識別，進而獲得該使用者可存取資源的存取權。一般而言，只有低階的驗證服務需要此權限。在預設狀況下並沒有定義任何安全性群組；因此，此使用者權限對於舊版用戶端和企業用戶端環境已夠用。不過，在高安全性環境中，則將此設定值設為「Revoke all security groups and accounts(撤銷所有安全性群組及帳戶)」。

新增工作站到網域中

表 3.22：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
未定義	未定義	未定義	管理員

Add workstations to domain (新增工作站到網域) 使用者權限允許使用者新增電腦到特定網域中。要讓這個權限發生作用，它必須指定給使用者作為網域「預設網域控制站原則」的一部份。在預設狀況下，並沒有定義任何安全性群組；因此，這項使用者權限對於舊版用戶端和企業用戶端環境已經足夠。不過，在高安全性系統環境中，要將此設定值設為僅將此使用者權限授與「Administrators(系統管理員)」群組。

調整處理序的記憶體配額

表 3.23：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員、 NETWORK SERVICE、 LOCAL SERVICE	未定義	未定義	管理員、 NETWORK SERVICE、 LOCAL SERVICE

Adjust memory quotas for a process (調整處理序的記憶體配額) 使用者權限可讓使用者將處理序的可用最大記憶體做調整。此權限適用於系統做微調時使用，但它也可能被濫用。在居心不良者手中，此使用者權限可用來啟動 DoS 攻擊。此使用者權限的預設安全性群組對於舊版用戶端和企業用戶端環境已夠用。不過，在高安全性環境中，則必須將此使用者權限設成強制使用「Administrators」、「NETWORK SERVICE」及「LOCAL SERVICE」值。

允許本機登入

表 3.24：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員、備份操作員、 Power Users 與使用者	管理員、備份操作員、 Power Users	管理員、備份操作員、 Power Users	管理員、備份操作員、 Power Users

Allow log on locally (允許本機登入) 使用者權限可決定哪些使用者可以相互登入至指定的電腦中。若要以 CTRL+ALT+DEL 組合鍵來啟動登入，使用者需擁有此登入權限。擁有此使用者權限的任意帳戶可用來登入電腦的本機主控台。請將此權限指定給真正需要登入到系統中的合法使用者，以防止未被授權的使用者提高其權限，或將病毒引入到運算系統環境中。

允許透過終端機服務登入

表 3.25：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員和遠端桌面使用者	管理員和遠端桌面使用者	管理員和遠端桌面使用者	管理員

Allow log on through Terminal Services (允許透過終端機服務登入) 使用者權限可決定哪些使用者或群組有權登入成為終端機服務用戶端。此使用者權限的預設安全性群組對於舊版用戶端和企業用戶端環境就已夠用。不過，在高安全性環境中，應該只有「(Administrators)系統管理員」可登入成為終端機服務用戶端。

變更系統時間

表 3.26：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員與 Power Users	未定義	未定義	管理員

Change the system time (變更系統時間) 使用者權限可決定哪些使用者和群組可變更電腦內部時鐘的時間和日期。擁有此使用者權限的使用者可影響事件記錄檔的外觀，因為事件記錄檔將反映新的時間，而非事件發生的實際時間。請將「Change the system time (變更系統時間)」權限只授與有正當理由來變更時間的使用者，例如 IT 部門的成員。若本機電腦和網域控制站的時間不同，Kerberos 驗證通訊協定可能會出問題，導致使用者無法登入至網域，或在登入之後無法取得授權來存取網域資源。

偵錯程式

表 3.27：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員	取消所有的安全性 群組和帳戶	取消所有的安全性 群組和帳戶	取消所有的安全性 群組和帳戶

Debug programs (偵錯程式) 使用者權限決定哪些使用者可將偵錯程式附加到任何處理序或核心內。此使用者權限可讓您完整地存取敏感和重要的作業系統元件。程式偵錯不應在實際執行環境中執行，除非是在很特別的環境內，例如在替無法有效存取測試環境中關鍵性商務應用程式解決問題時。

拒絕從網路存取此電腦

表 3.28：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
SUPPORT_388945a0	ANONYMOUS LOGON; 內建管理員; Guests; Support_388945a0; Guest; 所有非作業系統服務的帳戶	ANONYMOUS LOGON; 內建管理員; Guests; Support_388945a0; Guest; 所有非作業系統服務的帳戶	ANONYMOUS LOGON; 內建管理員; Guests; Support_388945a0; Guest; 所有非作業系統服務的帳戶

注意：ANONYMOUS LOGON、內建管理員、Support_388945a0、Guest 和所有非作業系統服務的帳戶都未包含於 .inf 安全性範本內。對於您組織內的每個網域，這些帳戶和群組都有唯一的安全性識別碼 (SID)。因此，它們必須手動地加入。如需進一步資訊，請參閱本章最後的「手動強化程序」。

Deny access to this computer from the network (拒絕從網路存取此電腦) 使用者權限可決定哪些使用者無法存取網路上的電腦。此使用者權限將拒絕許多網路通訊協定，包括了 SMB 型態的通訊協定、NetBIOS、CIFS、HTTP 和 COM+。當使用者帳戶受制於兩個原則時，此原則設定會蓋過「Deny access to this computer from the network (拒絕從網路存取此電腦)」使用者權限。若您設定其他群組擁有此登入權限，將可能會限制住在您的環境中被指定擁有特定管理角色的使用者的能力。記得確認委派的工作不會受到負面的影響。

拒絕登入成批次工作

表 3.29：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
未定義	Guests; Support_388945a0; Guest	Guests; Support_388945a0; Guest	Guests; Support_388945a0; Guest

注意：ANONYMOUS LOGON、內建管理員、Support_388945a0、Guest 和所有非作業系統服務的帳戶都未包含於 .inf 安全性範本內。對於您組織內的每個網域，這些帳戶和群組都有唯一的安全性識別碼 (SID)。因此，它們必須手動地加入。如需進一步資訊，請參閱本章最後的「手動強化程序」。

Deny log on as a batch job (拒絕登入成批次工作) 使用者權限可決定哪些帳戶不能登入至系統中進行批次工作。批次工作並非批次檔 (bat) – 它是一個批次 – 佇列設施。利用「Task Scheduler」排程工作的帳戶就需要此權限。此「Deny log on as a batch job (拒絕登入成批次工作)」使用者權限設定會蓋過「Log on as a batch job (登入成批次工作)」使用者權限設定。具有此登入權限的帳戶可用來排程工作，而這些工作可能會消耗大量系統資源，進而導致 DoS 的狀況發生。基於此理由，若不將「Deny log on as a batch job (拒絕登入成批次工作)」使用者權限指定給建議的帳戶，便可能會造成安全上的風險。

拒絕經由終端機服務登入

表 3.30：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
未定義	內建管理員; Guests; Support_388945a0; Guest; 所有非作業系統服務的 帳戶	內建管理員; Guests; Support_388945a0; Guest; 所有非作業系統服務的 帳戶	內建管理員; Guests; Support_388945a0; Guest; 所有非作業系統服務的 帳戶

注意：ANONYMOUS LOGON、內建管理員、Support_388945a0、Guest 和所有非作業系統服務的帳戶都未包含於 .inf 安全性範本內。對於您組織內的每個網域，這些帳戶和群組都有唯一的安全性識別碼 (SID)。因此，它們必須手動地加入。如需進一步資訊，請參閱本章最後的「手動強化程序」。

Deny log on through Terminal Services (拒絕經由終端機服務登入) 使用者權限可決定禁止哪些使用者和群組登入到 Terminal Services 用戶端。當您將基礎成員伺服器加入網域環境之後，並不需要使用本機帳戶從網路存取伺服器。網域帳戶便可透過存取伺服器來進行管理及終端使用者的處理。請記住，MSBP 要等到伺服器加入到網域中，並重新啟動兩次之後，才會收到此群組原則。因此，使用本機管理員帳戶是禁止的。

啓用電腦和使用者帳戶能信任作委派

表 3.31：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
未定義	未定義	未定義	取消所有的安全性群組和帳戶

Enable computer and user accounts to be trusted for delegation (啓用電腦和使用者帳戶能信任作委派) 使用者權限允許使用者變更 Active Directory 中使用者或電腦物件的「Trusted for Delegation (信任作委派)」設定。被授與此權限的使用者或電腦也必須擁有該物件的帳戶控制旗標的寫入存取權。濫用此權限，將可能導致未授權的使用者假冒網路上其他使用者的身份進入。

從遠端系統強迫關機

表 3.32：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員	未定義	未定義	管理員

Force shutdown from a remote system (從遠端系統強迫關機) 使用者權限可讓使用者從網路上的遠端位置關閉電腦。能夠關閉電腦的任何使用者都可能造成 DoS 的狀況發生；因此，此權限應該嚴格地限制。

產生安全性稽核

表 3.33：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
NETWORK SERVICE、 LOCAL SERVICE	未定義	未定義	NETWORK SERVICE、 LOCAL SERVICE

Generate security audits (產生安全性稽核) 使用者權限可讓處理序在安全性記錄檔中產生稽核記錄。安全性記錄檔可用來追蹤未授權的系統存取。寫入安全性記錄檔的帳戶可能會被駭客利用，在記錄檔內填入無意義的事件。若電腦設成依需要覆寫事件，駭客可使用此法來移除其未授權活動的證據。若電腦設定成在無法寫入安全性記錄檔時即關機，此方法也可讓DoS的狀況發生。

在驗證後模擬用戶端

表 3.34：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
SERVICE, Administrators	未定義	未定義	Local Service; Network Service

若指定 Impersonate a client after authentication(在驗證後模擬用戶端)權限，應用程式以使用者的身份去執行，並模擬用戶端。基於這類模擬來要求這個使用者權限，可防止未授權的使用者說服用戶端透過 – 例如遠端程序呼叫或具名管道 – 來連至他建立的某個服務並模擬該用戶端，之後再將未授權使用者的權限提高到管理或系統的層次。這個使用者權限的預設安全性群組已經能夠滿足舊版用戶端和企業用戶端系統環境的需求。

不過，在高安全性環境中要將此使用者權限設成「Local Service, NETWORK SERVICE」。

增加排程優先權

表 3.35：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員	未定義	未定義	管理員

Increase scheduling priority (增加排程優先權) 權限可讓使用者增加處理序的基礎優先權類別。增加優先權類別內的相對優先權並非授權的作業。作業系統所提供的管理工具並不需要此權限，但是軟體開發工具可能需要。擁有此權限的使用者若將處理序的排程優先權增加為「Real-Time」，如此其他的處理序就只有一點處理時間可用，進而導致 DoS 狀況。此使用者權限的預設安全性群組對於舊版用戶端和企業用戶端環境已很夠用。不過，在高安全性環境中，則必須將此使用者權限設定成強制使用預設的「Administrators(系統管理員)」群組。

載入和卸載裝置驅動程式

表 3.36：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員	未定義	未定義	管理員

Load and unload device drivers (載入和卸載裝置驅動程式) 權限決定哪些使用者可以動態地載入和卸載裝置驅動程式。若新硬體的簽章驅動程式已存在於電腦上的 Driver.cab 檔內，就不需要此權限。裝置驅動程式將可執行高權限的程式碼。被授與 Load and unload device drivers 權限的使用者可能會因此無心地安裝了偽裝成裝置驅動程式的惡意程式碼。但通常系統管理員應該會比較小心，並且只會安裝具有已確認數位簽章的驅動程式。此權限的預設使用者群組對於舊版用戶端和企業用戶端環境已夠用。不過，在高安全性環境中，則必須將此使用者權限設定成強制使用預設的「Administrators(系統管理員)」群組。

鎖定記憶體中的分頁

表 3.37：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
未定義	未定義	未定義	管理員

Lock pages in memory (鎖定記憶體中的分頁) 使用者權限可讓處理序將資料保存在實體記憶體內，這可防止系統將資料分頁放到磁碟上的虛擬記憶體內。啟用此使用者權限很可能會大幅降低系統的性能。擁有此權限的使用者可指定給予實體記憶體多個處理序，並留下極少或完全沒有隨機存取記憶體 (RAM) 給其他處理序。這也可能導致 DoS 狀況。此使用者權限的預設安全性群組對於舊版用戶端和企業用戶端環境已很夠用。不過，在高安全性環境中，則必須將此使用者權限設定成強制使用預設的「Administrators(系統管理員)」群組。

登入成批次工作

表 3.38：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
SUPPORT_388945a0、 LOCAL SERVICE	未定義	未定義	取消所有的安全性群組 和帳戶

Log on as a batch job (登入成批次工作) 使用者權限可讓使用者使用批次佇列設施 (例如 Task Scheduler 服務) 來登入。這是一個低風險的漏洞，因此，此使用者權限的預設值對於大多數的公司就已足夠。此使用者權限的預設安全性群組對於舊版用戶端和企業用戶端環境已很夠用。不過，在高安全性環境中，則應將此使用者權限設成「Revoke all security groups and accounts (取消所有的安全性群組與帳戶)」。

管理稽核與安全性記錄檔

表 3.39：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員	未定義	未定義	管理員

Manage auditing and security log (管理稽核與安全性記錄檔) 權限可讓使用者替個別的資源 (例如檔案、Active Directory 物件和登錄機碼) 指定物件存取稽核選項。管理安全性事件記錄檔的權限是一個強大的使用者權限，因此應該嚴加保護。任何擁有此使用者權限的人都可清除安全性記錄檔，因此可能刪除重要的未授權活動證據。此使用者權限的預設安全性群組對於舊版用戶端和企業用戶端環境已很夠用。不過，在高安全性環境中，則必須將此使用者權限設定成強制使用預設的「Administrators(系統管理員)」群組。

修改韌體環境值

表 3.40：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員	未定義	未定義	管理員

Modify firmware environment values (修改韌體環境值) 使用者權限可讓處理序透過 API 或使用者透過 System Properties 來修改系統環境變數。擁有此權限的任何人都可設定硬體元件的設定值來令它失敗，這可能導致資料損毀或 DoS 狀況。此使用者權限的預設安全性群組對於舊版用戶端和企業用戶端環境已很夠用。不過，在高安全性環境中，則必須將此使用者權限設定成強制使用預設的「Administrators(系統管理員)」群組。

執行磁碟區維護工作

表 3.41：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員	未定義	未定義	管理員

Perform volume maintenance tasks (執行磁碟區維護工作) 使用者權限可讓非管理或遠端的使用者管理磁碟區或磁碟。擁有此權限的使用者可刪除磁碟區，導致資料遺失或 DoS 狀況。此使用者權限的預設安全性群組對於舊版用戶端和企業用戶端環境已很夠用。不過，在高安全性環境中，則必須將此使用者權限設定成強制使用預設的「Administrators(系統管理員)」群組。

設定檔單一處理序

表 3.42：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員與 Power Users	未定義	未定義	管理員

Profile single process (設定檔單一處理序) 使用者權限可決定哪些使用者可使用效能監視工具來監視非系統處理序的效能。這是一個中度的漏洞；擁有此權限的駭客可監視電腦的效能，以找出可直接攻擊的關鍵處理序。駭客也可判斷什麼處理序正執行於系統上，以找出要防止哪些反制措施 – 例如防毒軟體、侵入偵測系統或其他登入至系統的使用者。要更妥善地保護環境，請在高安全性環境中，必須將 **Power Users** 從此使用者權限內移除。

設定檔系統效能

表 3.43：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員	未定義	未定義	管理員

Profile system performance (設定檔系統效能) 使用者權限可讓使用者監視系統處理序的效能。不限制此使用者權限將會出現一個中度的漏洞；擁有此權限的駭客可監視電腦的效能，以找出可直接攻擊的關鍵處理序。駭客也可判斷什麼處理序正執行於系統上，以找出要防止哪些反制措施 – 例如防毒軟體或侵入偵測系統。此使用者權限的預設安全性群組對於舊版用戶端和企業用戶端環境已很夠用。不過，在高安全性環境中，則必須將此使用者權限設定成強制使用預設的「Administrators(系統管理員)」群組。

從停駐站中移除電腦

表 3.44：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員、Power Users	未定義	未定義	管理員

Remove computer from docking station (從停駐站中移除電腦) 使用者權限可讓可攜式電腦的使用者按一下 [Start] 功能表中的 [Eject PC] 來移除電腦的停駐狀態。任何擁有此使用者權限的使用者都可移除已從其停駐站開機的可攜式電腦。此使用者權限的預設安全性群組對於舊版用戶端和企業用戶端環境已很夠用。不過，在高安全性環境中，則必須將此使用者權限設定成強制使用預設的「Administrators(系統管理員)」群組。

取代處理序層級的權杖

表 3.45：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
LOCAL SERVICE、 NETWORK SERVICE	未定義	未定義	LOCAL SERVICE、 NETWORK SERVICE

Replace a process level token (取代處理序層級的權杖) 使用者權限可讓父代處理序取代子處理序的相關存取權杖。此使用者權限的預設安全性群組對於舊版用戶端和企業用戶端環境已很夠用。不過，在高安全性環境中，則須將此使用者權限設成強制使用預設的 LOCAL SERVICE 與 NETWORK SERVICE 群組。

還原檔案與目錄

表 3.46：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員與備份操作員	未定義	管理員	管理員

Restore files and directories (還原檔案與目錄) 使用者權限可決定在還原備份的檔案和目錄時，哪些使用者可略過檔案、目錄、登錄和其他的永續性物件權限。它也會決定哪些使用者可將任何有效的安全性主角設成物件的擁有者。在企業或高安全性環境中，應該只有「Administrators(系統管理員)」有權還原檔案和目錄。還原檔案的工作通常是由管理員或另一個特別委派的安全性群組來執行，對於高度敏感的伺服器和網域控制站更是如此。

關閉系統

表 3.47：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
備份操作員、Power Users、管理員	未定義	管理員	管理員

Shut down the system (關閉系統) 使用者權限可決定哪些登入至本機的使用者可使用「Shut Down」指令來關閉作業系統。誤用此使用者權限可能導致 DoS 的攻擊。關閉網域控制站的能力應只有極少數的受信任管理員能夠擁有。即使系統關機需要能夠登入至伺服器的能力，您仍應對允許關閉網域控制站的帳戶和群組格外小心。在高安全性的環境中，應該只有「Administrators(系統管理員)」可授與「Shut down the system (關閉系統)」使用者權限。

同步化目錄服務資料

表 3.48：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
未定義	未定義	未定義	取消所有的安全性群組和帳戶

Synchronize directory service data (同步化目錄服務資料) 使用者權限可允許一個處理序讀取目錄內所有的物件和屬性，不管物件和屬性是否受到保護。使用者需擁有此權限，方能使用 LDAP 目錄同步化 (Dirsync) 服務。系統的預設值並未指定任何帳戶；不過，在高安全性環境中則須將此使用者權限設成「撤銷所有安全性群組及帳戶(Revoke all security groups and accounts)」。

運用檔案或其他物件的擁有權

表 3.49：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員	未定義	未定義	管理員

Take ownership of files or other objects (運用檔案或其他物件的擁有權) 使用者權限可讓使用者取得系統中任何可取得物件的擁有權，包括 Active Directory 物件、NTFS 檔案系統 (NTFS) 檔案和資料夾、印表機、登錄機碼、服務、處理序和執行緒。請確認只有本機「Administrators(系統管理員)」群組可擁有「Take ownership of files or other objects (運用檔案或其他物件的擁有權)」的使用者權限。

安全性選項

群組原則的 Security Options (安全性選項) 區可用來設定電腦的安全性設定，例如資料的數位簽章、系統管理員(Administrator) 和訪客(Guest) 帳戶名稱、軟式磁碟機和 CD-ROM 光碟機的存取、驅動程式安裝行為以及登入提示。

在 Windows Server 2003 中，Security Options 設定值可以在「群組原則物件編輯器」(Group Policy Object Editor) 的下列位置中設定：

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

並非所有的安全性群組都存在於所有的系統類型中。此外，許多您企業的網域間都只有單一安全性群組 SID。因此，群組原則的安全性選項部分可能需要手動地修改於目標群組所在的系統內。本節詳述了在 MSBP 中，本手冊所定義三個系統環境的預定安全性選項。如需本節所預定的設定摘要，請參閱 Windows Server 2003 Security Guide Settings Excel 工作簿。如需預設設定的相關資訊，及此節所討論的每個設定的詳細說明資訊，請參閱所附手冊《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》，網址為：<http://go.microsoft.com/fwlink/?LinkId=15159>。

帳戶：Guest 帳戶狀態

表 3.50：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	停用	停用

Accounts:Guest account status (帳戶：Guest 帳戶狀態) 安全性選項設定值可決定訪客 (Guest) 帳戶是啟用或停用。此帳戶可讓未驗證的網路使用者透過Guest 來登入並存取系統。因此，此安全性選項設定值在三個系統環境中都應設成停用 (Disabled)。

帳戶：將空白密碼的本機帳戶使用限制只能登入主控台

表 3.51：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
啟用	啟用	啟用	啟用

Accounts:Limit local account use of blank passwords to console logon only (帳戶：將空白密碼的本機帳戶使用限制只能登入主控台) 安全性選項設定值可決定未受密碼保護的本機帳戶可否從實體電腦主控台以外的位置登入。啟用此設定可防止擁有非空白密碼的本機帳戶從遠端用戶端登入到網路，同時未受密碼保護的本機帳戶，只能透過電腦的鍵盤實體地登入。因此，請將此反制措施的預設值強制在三個系統環境中執行。

稽核：稽核全域系統物件的存取

表 3.52：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	停用	停用

Audit:Audit the access of global system objects (稽核：稽核全域系統物件的存取) 安全性選項設定值可在全域系統物件生效時，稽核其存取。若同時啟用「Audit:Audit the access of global system objects(稽核：稽核全域系統物件的存取)」和「Audit object access audit policy(稽核物件存取稽核原則)」這兩個設定，將會產生大量的稽核事件。本手冊所定義的三個系統環境都將此選項設成預設值。

注意：您必須重新啟動 Windows Server 2003，此安全性選項設定值的組態變更才會生效。

稽核：稽核備份與還原權限的使用

表 3.53：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	停用	停用

Audit:Audit the use of Backup and Restore privilege (稽核：稽核備份與還原權限的使用) 安全性選項設定值可決定當 Audit privilege use(稽核權限使用) 原則設定生效時，是否要稽核所有使用者權限的使用，包括了 Backup and Restore (備份與還原)。啟用此原則可能會產生大量的安全性事件，導致伺服器回應速度變慢，並強迫安全性事件記錄檔記錄許多不重要的事件。因此，本手冊所定義的三個系統環境都將此選項設成預設值。

注意：您必須重新啟動 Windows Server 2003，此安全性選項設定值的組態變更才會生效。

稽核：若無法記錄安全性稽核就立即關閉系統

表 3.54：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	停用	啟用

Audit:Shut down system immediately if unable to log security audits (稽核：若無法記錄安全性稽核就立即關閉系統) 安全性選項設定值將決定若系統無法記錄安全性事件，是否要立即關機。由於在舊版用戶端和企業用戶端環境中啟用此設定所需的額外管理負荷量太高了，因此群組原則會將「Shut down system immediately if unable to log security audits(稽核：若無法記錄安全性稽核就立即關閉系統)」設定值設成停用(Disabled)。不過，高安全性環境則將此選項設成啟用，因為要防止他人從安全性事件記錄檔中刪除事件，這額外的管理負荷量是可接受的。

裝置：允許毋須登入即取消停駐

表 3.55：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
啟用	停用	停用	停用

Devices：Allow undock without having to log on (裝置：允許毋須登入即取消停駐) 安全性選項設定值可決定可攜式電腦可否在使用者未登入至系統，便即取消停駐。啟用此設定可去除登入需求，並允許透過外部的硬體彈出按鈕來取消電腦的停駐狀態。停用此設定意味著使用者必須被授與 Remove computer from docking station (從停駐站中移除電腦) 使用者權限 (未定義於本手冊內)，方能在不登入至系統時取消電腦的停駐狀態。

裝置：允許格式化與取出抽取式媒體

表 3.56：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員	管理員	管理員	管理員

Devices:Allowed to format and eject removable media (裝置：允許格式化與彈出抽取式媒體) 安全性選項設定值可決定誰可格式化與取出抽取式媒體。應該只有系統管理員可取出伺服器上的抽取式媒體。因此，此設定值的反制措施為本手冊所定義三個系統環境中的預設值。

裝置：防止使用者安裝印表機驅動程式

表 3.57：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
啟用	啟用	啟用	啟用

若電腦想印到網路印表機上，就必須先安裝該網路印表機的驅動程式。啟用 Devices:Prevent users from installing printer drivers (裝置：防止使用者安裝印表機驅動程式) 安全性選項設定值只允許 Administrators 或 Power Users 群組內的使用者，或擁有 Server Operator 權限的使用者安裝印表機驅動程式，作為新增網路印表機的一部份。若停用此設定，任何使用者都可安裝印表機驅動程式，作為新增網路印表機的一部份。此設定值的反制措施為本手冊所定義三個系統環境中的預設值。

裝置：限制只有本機登入的使用者可存取 CD-ROM

表 3.58：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	未定義	未定義	啟用

Devices:Restrict CD-ROM access to locally logged-on user only (裝置：限制只有本機登入的使用者可存取 CD-ROM) 安全性選項設定值可決定本機和遠端的使用者是否可同時存取 CD-ROM。啓用此設定只允許以互動方式登入的使用者可讀取抽取式 CD-ROM 媒體。若啓用此原則，並且沒有任何人是以互動方式登入，CD-ROM 將可存取於網路上。在舊版用戶端和企業用戶端環境中，此值將設成「未定義Not Defined」。在高安全性環境中，此值則設成「啓用(Enabled)」。

裝置：限制只有本機登入的使用者可存取磁片

表 3.59：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	未定義	未定義	啓用

Devices:Restrict floppy access to locally logged-on user only (裝置：限制只有本機登入的使用者可存取磁片) 安全性選項設定值可決定本機和遠端的使用者是否可同時存取磁片媒體。若啓用這設定，只有以互動方式登入的使用者可存取抽取式磁片媒體。若啓用此原則，並且沒有任何人是以互動方式登入，磁片媒體便可透過網路來存取。在舊版用戶端和企業用戶端環境中，請將此值設成停用(Disabled)。在高安全性環境中，則將此值設成啓用(Enabled)。

裝置：未簽章的驅動程式安裝行爲

表 3.60：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
警告但允許安裝	警告但允許安裝	警告但允許安裝	警告但允許安裝

Devices:Unsigned driver installation behavior (裝置：未簽章的驅動程式安裝行爲) 安全性選項設定值可決定當有人嘗試安裝某個未經核准、且未由 Windows Hardware Quality Lab (WHQL) 簽章過的裝置驅動程式時 (透過 Setup API) 會發生何事。此選項可防止他人安裝未簽章過的驅動程式，或警告管理員有一個未簽章的驅動程式正要安裝。這可防止他人安裝未經認證可執行於 Windows Server 2003 上的驅動程式。將此設定值設成「警告但可安裝(Warn but allow installation)」的一個潛在問題是，自動安裝指令碼在安裝未簽章的驅動程式時將會失敗。

網域控制站：允許伺服器操作員排程工作

表 3.61：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
未定義	停用	停用	停用

Domain controller:Allow server operators to schedule tasks (網域控制站：允許伺服器操作員排程工作) 安全性選項設定值可決定伺服器操作員可否透過 AT 排程機制來送出工作。本手冊所定義的三個系統環境都將此選項設成停用。停用此設定的影響對於大多數的組織而言，應該都很小。使用者，包括了在 Server Operators 群組內的使用者，仍可透過 Task Scheduler Wizard 來建立工作，但是這些工作將在使用者建立該工作時用來驗證的帳戶環境中執行。

注意：AT 服務帳戶可加以修改，以便選取不同於 LOCAL SYSTEM 帳戶的帳戶。若要變更帳戶，請開啓 System Tools、按一下 Scheduled Tasks、之後按一下 Accessories 資料夾。接著按 Advanced 功能表中的 AT Service Account。

網域控制站：LDAP 伺服器簽章需求

網域控制站LDAP 伺服器簽章需求

表 3.62：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
未定義	未定義	未定義	需要簽章

Domain controller:LDAP server signing requirements (網域控制站：LDAP 伺服器簽章需求) 安全性選項設定值可決定 LDAP 伺服器是否需要簽章，方能與 LDAP 用戶端進行交涉。既未簽章、又未加密的網路傳輸極容易遭受中間人攻擊 (Man-in-the-Middle Attack)，也就是侵入者在伺服器 and 用戶端之間攔截封包，並在將它們傳給用戶端之前加以修改。就 LDAP 伺服器的狀況而言，這意味著駭客可令用戶端根據來自 LDAP 目錄的錯誤記錄做決定。若所有的網域控制站都執行 Windows 2000 (含) 以後版本，請將此安全性選項設成需要簽章(Require signing)。否則，將此設定保留為未定義(Not Defined)。因為高安全性環境中的所有電腦不是執行 Windows 2000，就是執行 Windows Server 2003，此環境會將此設定設成需要簽章 (Require signing)。

網域控制站：拒絕機器帳戶密碼的變更

表 3.63：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
未定義	停用	停用	停用

Domain controller:Refuse machine account password changes (網域控制站：拒絕機器帳戶密碼的變更) 安全性選項設定值可決定網域控制站可否拒絕來自成員電腦的變更電腦帳戶密碼要求。在某個網域的所有網域控制站上啟用此設定，會令網域成員的電腦帳戶密碼無法變更，令它們容易受到攻擊。因此，在本手冊定義的三個系統環境中，都將此安全性選項的值設成停用(Disabled)。

網域成員：替安全通道資料數位加密或簽章 (每次)

表 3.64：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
啟用	停用	停用	啟用

Domain member:Digitally encrypt or sign secure channel data (always) (網域成員：替安全通道資料數位加密或簽章 (每次)) 安全性選項設定值可決定網域成員所啓始的所有安全通道傳輸資料是否都必須簽章或加密。若某系統設成必須替安全通道資料加密或簽章，那它就無法以無法替所有安全通道傳輸簽章或加密的網域控制站來建立安全通道，因為所有安全通道資料都已簽章和加密。舊版用戶端和企業用戶端環境將此安全性選項設成停用(Disabled)，而高安全性環境則將它設成啟用(Enabled)。

注意：若要在成員工作站和伺服器上運用此安全性選項設定值，所有組成成員網域的網域控制站都必須執行 Windows NT 4.0 搭配 Service Pack 6a 或以後版本；Windows 98 Second Edition 用戶端就不支援此選項 (除非它們安裝了 dsclient)。

網域成員：替安全通道資料數位加密 (可能的話)

表 3.65：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
啟用	啟用	啟用	啟用

Domain member:Digitally encrypt secure channel data (when possible) (網域成員：替安全通道資料數位加密 (可能的話)) 安全性選項設定值可決定網域成員可否嘗試更動自己啓始之所有安全通道傳輸的加密。啟用此設定可令網域成員要求所有安全通道傳輸的加密。停用此設定可禁止網域成員更動安全通道加密。因此，本手冊所定義的三個系統環境都將此選項設成啟用(Enabled)。

網域成員：替安全通道資料加入數位簽章 (可能的話)

表 3.66：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
啟用	啟用	啟用	啟用

Domain member:Digitally sign secure channel data (when possible) (網域成員：替安全通道資料加入數位簽章 (可能的話)) 安全性選項設定值可決定網域成員可否嘗試更動自己啓始之所有安全通道傳輸的簽章。簽章可防止傳輸資料在半路上被任何攔截資料的人修改。本手冊所定義的三個系統環境都將此設定設成啟用(Enabled)。

網域成員：停用機器帳戶密碼變更

表 3.67：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	停用	停用

Domain member:Disable machine account password changes (網域成員：停用機器帳戶密碼變更) 安全性選項設定值可決定網域成員可否定期變更其電腦帳戶密碼。啓用此設定可防止網域成員變更其電腦帳戶密碼。若停用此設定，網域成員可依照「Domain member:Disable machine account password changes (網域成員：停用機器帳戶密碼變更)」設定值所指定的天數來變更其電腦帳戶密碼，其預設值為每隔 30 天變更一次。若電腦不能自動變更其帳戶密碼，駭客就有可能找出系統網域帳戶的密碼。因此，在本手冊所定義的三個系統環境中，均將此反制措施設成停用(Disabled)。

網域成員：最大的機器帳戶密碼存留期

表 3.68：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
30 天	30 天	30 天	30 天

Domain member:Maximum machine account password age (網域成員：最大的機器帳戶密碼存留期) 安全性選項設定值可決定電腦帳戶密碼的最大可容許存留期。此設定值也適用於執行 Windows 2000 的電腦，但它並無法用於這些電腦的 Security Configuration Manager 工具。在預設狀態下，網域成員每隔 30 天就會自動變更其網域密碼。將此間隔值設得很大，或將它設成 0，讓電腦無法再變更其密碼，都會令駭客有更多時間對某個電腦帳戶進行暴力式 (Brute Force) 的密碼臆測攻擊。因此，本手冊所定義的三個系統環境都將此選項設成 30 天。

網域成員：需要強式 (Windows 2000 或以後版本) 工作階段金鑰

表 3.69：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	啓用	啓用	啓用

Domain member:Require strong (Windows 2000 or later) session key (網域成員：需要強式 (Windows 2000 或以後版本) 工作階段金鑰) 安全性選項設定值可決定加密的安全通道資料是否需要 128-bit 金鑰強度。啓用此設定可防止建立不含 128-bit 加密的安全通道。若停用此設定，網域成員必須和網域控制站交涉金鑰強度。在 Windows 2000 中，用來在網域控制站和成員電腦之間建立安全通道通訊的工作階段金鑰遠比在先前的 Microsoft 作業系統強。因此，由於本手冊所述三個安全性環境都包含 Windows 2000 網域控制站(含) 以後的版本，此三個系統環境都將此設定設成啓用(Enabled)。

注意：若您在 Windows NT 4.0 網域中啓用此設定，您將無法聯結執行 Windows 2000 的電腦。

互動式登入：不顯示最後的使用者名稱

表 3.70：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	啓用	啓用	啓用

Interactive logon:Do not display last user name (互動式登入：不顯示最後的使用者名稱) 安全性選項設定值可決定最後登入至電腦的使用者名稱是否要顯示於 Windows 登入螢幕上。啓用此設定可防止將最後登入的使用者名稱顯示在「Log On to Windows」對話方塊內。互動式登入(Interactive logon):本手冊所定義三個系統環境中的基礎伺服器原則都將「Do not display last user name(不要顯示最後使用者的名稱)」選項設成啓用。

互動式登入:不需要 CTRL+ALT+DEL

表 3.71：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	停用	停用

Interactive logon:Do not require CTRL+ALT+DEL(互動式登入:不需要CTRL+ALT+DEL) 安全性選項設定值可決定在使用者在登入之前是否需按 CTRL+ALT+DEL。若停用此設定，所有使用者都必須按 CTRL+ALT+DEL，才能登入至 Windows (除非他們使用智慧卡來進行 Windows 登入)。本手冊所定義的三個系統環境都將此設定設成停用(Disabled)，以減少駭客透過 Trojan 木馬程式來攔截使用者密碼的機會。

互動式登入：使用者嘗試登入時的訊息文字

表 3.72：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
未定義	This system is restricted to authorized users. (此系統侷限於授權的使用者。)Individuals attempting unauthorized access will be prosecuted.(嘗試未授權存取的个人將會遭起訴。)If unauthorized, terminate access now!(若未經授權，就立即終止存取！)Clicking on OK indicates your acceptance of the information in the background.(按一下 OK，代表您接受背景所示的資訊。)	This system is restricted to authorized users. (此系統侷限於授權的使用者。)Individuals attempting unauthorized access will be prosecuted.(嘗試未授權存取的个人將會遭起訴。)If unauthorized, terminate access now!(若未經授權，就立即終止存取！)Clicking on OK indicates your acceptance of the information in the background.(按一下 OK，代表您接受背景所示的資訊。)	This system is restricted to authorized users. (此系統侷限於授權的使用者。)Individuals attempting unauthorized access will be prosecuted.(嘗試未授權存取的个人將會遭起訴。)If unauthorized, terminate access now!(若未經授權，就立即終止存取！)Clicking on OK indicates your acceptance of the information in the background.(按一下 OK，代表您接受背景所示的資訊。)

Interactive logon:Message text for users attempting to log on (互動式登入：使用者嘗試登入時的訊息文字) 安全性選項設定值將指定使用者登入時所要顯示的文字訊息。此文字通常用於合法性理由，例如警告使用者關於誤用公司資訊的結果，或警告他們其行為將會受到稽核。這三個系統環境都建議設定一段訊息文字。

注意：您顯示的任何警告都應先由您公司的法律和人力資源代表核准。此外，「Interactive logon:Message text for users attempting to log on」和「Interactive logon:Message title for users attempting to log on」這兩個設定值必須同時啓用，它們才能正常地運作。

互動式登入：使用者嘗試登入時的訊息標題

表 3.73：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
未定義	IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZATION (若無適當的授權，繼續執行將會違法)	IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZATION (若無適當的授權，繼續執行將會違法)	IT IS AN OFFENSE TO CONTINUE WITHOUT PROPER AUTHORIZATION (若無適當的授權，繼續執行將會違法)

Interactive logon:Message title for users attempting to log on (互動式登入：使用者嘗試登入時的訊息標題) 安全性選項設定值可替視窗的標題列指定標題，以供使用者登入至系統時檢視。使用此設定的原因就和使用「Message text for user attempting to log on」設定的原因一樣。不使用此設定的公司較容易受到專門攻擊網路表面的駭客所攻擊。因此，本手冊所定義三個系統環境都啓用此設定。

注意：您顯示的任何警告都應先由您公司的法律和人力資源代表核准。此外，「Interactive logon:Message text for users attempting to log on」和「Interactive logon:Message title for users attempting to log on」這兩個設定值必須同時啓用，它們才能正常地運作。

互動式登入：欲快取的先前登入個數 (萬一網域控制站無法使用的話)

表 3.74：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
10	1	0	0

Interactive logon: Number of previous logons to cache (in case domain controller is not available) (互動式登入：欲快取的先前登入個數 (萬一網域控制站無法使用的話)) 安全性選項設定值可決定使用者可否使用快取的帳戶資訊來登入 Windows 網域。網域帳戶的登入資訊可快取於本機，因此若無法在接下來的登入中聯繫上網域控制站，使用者仍可登入。此設定值可決定可將多少個不同的使用者登入資訊快取於本機。將此值設成 0 就會停用登入快取，這也是建議在本手冊定義的三個系統環境的的設定值。

互動式登入：在過期之前提示使用者變更密碼

表 3.75：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
14 天	14 天	14 天	14 天

Interactive logon: Prompt user to change password before expiration (互動式登入：在過期之前提示使用者變更密碼) 安全性選項設定值可決定要提前幾天警告使用者其密碼即將過期。本手冊的「帳戶原則」一節將建議您將使用者密碼設成會定期地過期。若使用者未在密碼即將過期前收到通知，他們會一直到密碼過期之後才得知此事。這可能會導致在本機存取網路的使用者迷糊，或令使用者無法透過撥號或虛擬私人網路 (VPN) 連線來存取您組織的網路。因此，本手冊所定義的三個系統環境都將此選項設成預設值 14 天。

互動式登入：需要網域控制站驗證來解除鎖定工作站

表 3.76：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	啟用	啟用	啟用

對於網域帳戶而言，Interactive logon:Require Domain Controller authentication to unlock workstation (互動式登入：需要網域控制站驗證來解除鎖定工作站) 安全性選項設定值可決定是否必須連上網域控制站，才能解除鎖定電腦。此設定值所解決的漏洞和「Interactive logon:Number of previous logons to cache (當網域控制站無法使用)」設定值類似。使用者可中斷接連伺服器的網路纜線，並解除鎖定使用舊密碼的伺服器，而不用透過驗證來解除鎖定該伺服器。因此，本手冊所定義的三個系統環境都將此選項設成啟用(Enabled)。

重要：此設定值也適用於執行 Windows 2000 或以後版本的電腦，但它並無法用於執行 Windows 2000 的電腦上的 Security Configuration Manager 工具 — 僅適合執行 Windows Server 2003 的電腦。

互動式登入：智慧卡移除行為

表 3.77：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
No Action	未定義	鎖定工作站	鎖定工作站

Interactive logon:Smart card removal behavior (互動式登入：智慧卡移除行為) 安全性選項設定值可決定當登入使用者的智慧卡從智慧卡讀取器中移除時會發生何事。若將此選項設成「Lock Workstation」，當使用者抽出智慧卡時，將會鎖定工作站，如此使用者若由於離開座位而取出智慧卡時，就可自動鎖定其工作站。若將此選項設成「Force Logoff」，當智慧卡移除時，系統會將使用者自動登出。

Microsoft 網路用戶端：替通訊加入數位簽章 (每次)

表 3.78：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	啟用	啟用

Microsoft network client:Digitally sign communications (always) (Microsoft 網路用戶端：替通訊加入數位簽章 (每次)) 安全性選項設定值可決定 SMB 伺服器元件是否需要封包簽章。啟用此設定可防止 Microsoft 網路用戶端與 Microsoft 網路伺服器進行通訊，除非伺服器同意執行 SMB 封包簽章。在舊版用戶端的混合環境中，請將此選項設成停用(Disabled)，因為這些用戶端並無法驗證或存取網域控制站。不過，您可在 Windows 2000 或以後版本的環境中使用此設定。本手冊所定義的企業用戶端和高安全性環境僅包含執行 Windows 2000 或以後版本的系統，它們都支援替通訊加入數位簽章。因此，若要在此環境內增加系統之間的通訊安全性，請將企業用戶端和高安全性環境中的此設定設成啟用(Enabled)。

Microsoft 網路用戶端：替通訊加入數位簽章 (伺服器同意的話)

表 3.79：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
啟用	啟用	啟用	啟用

Microsoft network client：Digitally sign communications (if server agrees) (Microsoft 網路用戶端：替通訊加入數位簽章 (伺服器同意的話)) 安全性選項設定值可決定 SMB 用戶端是否嘗試交涉 SMB 封包簽章。在 Windows 網路中實作數位簽章有助於防止工作階段被擷取。透過啟用此設定，成員伺服器上的 Microsoft 網路用戶端只會在所溝通的伺服器接受數位簽章之通訊時，才會要求簽章。本手冊所定義的三個系統環境都將此設定設成啟用(Enabled)。

Microsoft 網路用戶端：傳送未加密密碼給協力廠商 SMB 伺服器

表 3.80：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	停用	停用

若 Microsoft network client:Send unencrypted password to third-party SMB servers (Microsoft 網路用戶端：傳送未加密密碼給協力廠商 SMB 伺服器) 安全性選項設定值設成啟用，SMB 重新導向器可在驗證時，將純文字密碼傳給不支援密碼加密的非 Microsoft SMB 伺服器。在本手冊定義的三個系統環境中，此選項都設成預設值停用(Disabled)，除非應用程式的需求超越維護機密密碼的需求。

Microsoft 網路伺服器：暫停工作階段前所需的閒置時間長度

表 3.81：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
15 分鐘	15 分鐘	15 分鐘	15 分鐘

Microsoft network server：Amount of idle time required before suspending session (Microsoft 網路伺服器：暫停工作階段前所需的閒置時間長度) 安全性選項設定值可決定 SMB 工作階段必須經過多長的連續閒置時間，該工作階段才會由於無活動而暫停。系統管理員可使用此原則來控制電腦何時暫停無活動的 SMB 工作階段。若用戶端恢復活動，該工作階段就會自動重新建立。本手冊定義的三個系統環境都將此選項設成 15 分鐘。

Microsoft 網路伺服器：替通訊加入數位簽章 (每次)

表 3.82：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	啟用	啟用

Microsoft network server：Digitally sign communications (always) (Microsoft 網路伺服器：替通訊加入數位簽章 (每次)) 安全性選項設定值可決定 SMB 伺服器元件是否需要封包簽章，方能與 SMB 用戶端進一步地通訊。Windows 2000 Server、Windows 2000 Professional、Windows Server 2003 和 Windows XP Professional 包含了支援相互驗證的 SMB 版本，它會關閉工作階段劫取式攻擊，並支援訊息驗證 (進而防止中間人攻擊)。SMB 簽章提供此驗證的作法是，將數位簽章放到每個 SMB 封包內，接著由用戶端和伺服器來確認。當電腦設成忽略所有未簽章的 SMB 通訊時，舊版應用程式和作業系統將無法連線。完全停用所有的 SMB 簽章，將會使得電腦工作階段容易受到劫取式攻擊。

Microsoft 網路伺服器：替通訊加入數位簽章 (用戶端同意的話)

表 3.83：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	啟用	啟用	啟用

Microsoft network server:Digitally sign communications (if client agrees) (Microsoft 網路伺服器：替通訊加入數位簽章 (用戶端同意的話)) 安全性選項設定值可決定 SMB 伺服器是否會與要求它的用戶端交涉 SMB 封包簽章。Windows 2000 Server、Windows 2000 Professional、Windows Server 2003 和 Windows XP Professional 包含了支援相互驗證的 SMB 版本，它會關閉工作階段劫取式攻擊，並支援訊息驗證 (進而防止中間人攻擊)。SMB 簽章提供此驗證的作法是，將數位簽章放到每個 SMB 封包內，接著由用戶端和伺服器來確認之。當電腦設成忽略所有未簽章的 SMB 通訊時，舊版應用程式和作業系統將無法連線。完全停用所有的 SMB 簽章，將令電腦容易受到工作階段劫取式攻擊。

Microsoft 網路伺服器：登入小時過期後切斷與用戶端的連接

表 3.84：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
啟用	啟用	啟用	啟用

Microsoft network server:Disconnect clients when logon hours expire (Microsoft 網路伺服器：登入小時過期後切斷與用戶端的連接) 安全性選項設定值可決定當使用者在其使用者帳戶的有效登入小時之外連至網路電腦時，是否該切斷其連接。此設定值將會影響 SMB 元件。若您的組織已替使用者設定了登入小時，那啓用此原則才有意義；否則原本不能在登入小時之外存取網路資源的使用者，事實上卻可透過在許可的小時內建立的工作階段，持續使用這些資源。基於這些理由，本手冊所定義的三個系統環境都將此選項設成啓用(Enabled)。

網路存取：不允許匿名列舉 SAM 帳戶

表 3.85：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
啓用	啓用	啓用	啓用

Network access:Do not allow anonymous enumeration of SAM accounts (網路存取：不允許匿名列舉 SAM 帳戶) 安全性選項設定值可決定要以密碼方式連至電腦需被授與哪些額外的權限。本手冊所定義的三個系統環境都將此選項設成啓用(Enabled)。

網路存取：不允許匿名列舉 SAM 帳戶和共用區

表 3.86：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	啓用	啓用	啓用

Network Access:Do not allow anonymous enumeration of SAM accounts and shares (網路存取：不允許匿名列舉 SAM 帳戶和共用區) 安全性選項設定值可決定是否允許匿名列舉 SAM 帳戶和共用區。本手冊所定義的三個系統環境都將此選項設成啓用(Enabled)。

網路存取：不允許儲存網路驗證的憑證或 .NET Passport

表 3.87：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	啓用	啓用	啓用

Network Access:Do not allow storage of credentials or .NET Passports for network authentication (網路存取：不允許儲存網路驗證的憑證或 .NET Passport) 安全性選項設定值可決定在取得網域驗證之後，「Stored User Names and Passwords」的設定值是否會儲存密碼、憑證或 Microsoft .NET Passports，以供日後使用。本手冊所定義的三個安全性環境都將此選項設成啓用(Enabled)。

注意：在設定此安全性選項時，您必須重新啓動 Windows，所做的變更才會生效。

網路存取：讓 Everyone 權限套用至匿名使用者

表 3.88：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	停用	停用

Network access:Let Everyone permissions apply to anonymous users (網路存取：讓 Everyone 權限套用至匿名使用者) 安全性選項設定值可決定若要以匿名方式連至電腦，需要哪些額外的權限。若啟用此設定，匿名的 Windows 使用者將可執行某些活動，例如列舉網域帳戶和網路共用區的名稱。未被授權的使用者可以匿名方式列出帳戶名稱與共用的資源，並使用此資訊來臆測密碼或執行人因缺陷式攻擊 (Social Engineering Attack)。因此，本手冊所定義的三個系統環境都將此選項設成停用(Disabled)。

注意：擁有此設定的網域將無法與 Windows NT 4.0 網域或網域控制站建立或維護信任。

網路存取：無法以匿名方式存取的具名管道

表 3.89：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
未定義	無	無	無

Network access:Named Pipes that can be accessed anonymously (網路存取：無法以匿名方式存取的具名管道) 安全性選項設定值可決定哪些通訊工作階段 (具名管道) 可擁有容許匿名存取的屬性和權限。在企業用戶端和高安全性環境中，應將「Network access:Named Pipes that can be accessed anonymously」選項設成 None。

重要：若您需要啟用此設定，請確認您只加入支援您系統環境之應用程式式所需的具名管道。就和本手冊建議的所有設定值一樣，此設定值應該仔細地測試於您的實際執行環境中。

網路存取：可遠端存取的登錄路徑

表 3.90：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
System\CurrentControlSet\Control\	System\CurrentControlSet\Control\	System\CurrentControlSet\Control\	System\CurrentControlSet\Control\
Product Options; System\CurrentControlSet\Control\	Product Options; System\CurrentControlSet\Control\	Product Options; System\CurrentControlSet\Control\	Product Options; System\CurrentControlSet\Control\
Server Applications; Software\	Server Applications; Software\	Server Applications; Software\	Server Applications; Software\
Microsoft\Windows NT\Current Version	Microsoft\Windows NT\Current Version	Microsoft\Windows NT\Current Version	Microsoft\Windows NT\Current Version

Network access:Remotely accessible registry paths (網路存取：可遠端存取的登錄路徑) 安全性選項設定值可決定哪些登錄路徑可在網路上存取。建議您在本手冊所定義的三個安全性環境中都強制使用基礎安全性範本內的預設值。

注意：即使您設定此安全性選項，仍須啟動 Remote Registry (遠端登錄) 系統服務，才能讓授權的使用者在網路上存取登錄。

網路存取：可遠端存取的登錄路徑和子路徑

表 3.91：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
System\CurrentControlSet\Control\Print\Printers	System\CurrentControlSet\Control\Print\Printers	System\CurrentControlSet\Control\Print\Printers	System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\Services\Eventlog	System\CurrentControlSet\Services\Eventlog	System\CurrentControlSet\Services\Eventlog	System\CurrentControlSet\Services\Eventlog
Software\Microsoft\OLAP Server	Software\Microsoft\OLAP Server	Software\Microsoft\OLAP Server	Software\Microsoft\OLAP Server
Software\Microsoft\Windows NT\CurrentVersion\Print	Software\Microsoft\Windows NT\CurrentVersion\Print	Software\Microsoft\Windows NT\CurrentVersion\Print	Software\Microsoft\Windows NT\CurrentVersion\Print
Software\Microsoft\Windows NT\CurrentVersion\Windows	Software\Microsoft\Windows NT\CurrentVersion\Windows	Software\Microsoft\Windows NT\CurrentVersion\Windows	Software\Microsoft\Windows NT\CurrentVersion\Windows
System\CurrentControlSet\Control\ContentIndex	System\CurrentControlSet\Control\ContentIndex	System\CurrentControlSet\Control\ContentIndex	System\CurrentControlSet\Control\ContentIndex
System\CurrentControlSet\Control\Terminal Server	System\CurrentControlSet\Control\Terminal Server	System\CurrentControlSet\Control\Terminal Server	System\CurrentControlSet\Control\Terminal Server
System\CurrentControlSet\Control\Terminal	System\CurrentControlSet\Control\Terminal	System\CurrentControlSet\Control\Terminal	System\CurrentControlSet\Control\Terminal
System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration	System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration	System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration	System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib	Software\Microsoft\Windows NT\CurrentVersion\Perflib	Software\Microsoft\Windows NT\CurrentVersion\Perflib	Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog	System\CurrentControlSet\Services\SysmonLog	System\CurrentControlSet\Services\SysmonLog	System\CurrentControlSet\Services\SysmonLog

Network access:Remotely accessible registry paths and sub-paths (網路存取：可遠端存取的登錄路徑和子路徑) 安全性選項設定值可決定哪些登錄路徑和子路徑可在網路上存取。建議您在本手冊所定義的三個安全性環境中都強制使用基礎安全性範本內的預設值。

網路存取：限制匿名存取具名管道和共用區

表 3.92：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
啟用	啟用	啟用	啟用

當下列選項啟用時，Network access:Restrict anonymous access to Named Pipes and Shares (網路存取：限制匿名存取具名管道和共用區) 安全性選項設定值會將匿名存取限制成只能存取共用區和具名管道：

- Network access:Named pipes that can be accessed anonymously
- Network access:Shares that can be accessed anonymously

本手冊所定義的三個系統環境都將此選項設成預設值。

網路存取：可以匿名存取的共用區

表 3.93:設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
COMCFG,DFS\$	無	無	無

Network access:Shares that can be accessed anonymously (網路存取：可以匿名存取的共用區) 安全性選項設定值可決定哪些網路共用區可被匿名使用者所存取。此設定的預設值並沒有很大影響，因為所有使用者都必須通過驗證，才能存取伺服器上的共用資源。因此，請確認本手冊所定義的三個系統環境都將此選項設成 None。

注意：啓用此群組原則設定相當危險；因為所列的任何共用區都可被任何網路使用者所存取。這可能導致暴露或損毀敏感的共同資料。

網路存取：本機帳戶的共用與安全性模型

表 3.94：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Classic (一般) – 本機使用者將驗證成爲本身	Classic (一般) – 本機使用者將驗證成爲本身	Classic (一般) – 本機使用者將驗證成爲本身	Classic (一般) – 本機使用者將驗證成爲本身

Network access:Sharing and security model for local accounts (網路存取：本機帳戶的共用與安全性模型) 安全性選項設定值可決定使用本機帳戶的網路登入如何驗證。「Classic」設定可讓使用者微調資源的存取方式。使用「Classic」設定可讓您針對相同的資源，授與不同類的存取給不同的使用者。使用「Guest only」設定值可讓您一視同仁地對待所有的使用者。在此狀況下，驗證成「Guest only」的所有使用者對於同一給定資源都會收到相同的存取等級。因此，本手冊所定義的三個系統環境都採用「Classic」的預設選項。

網路安全性：當下次密碼更改時，不要儲存 LAN Manager 雜湊值

表 3.95：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	啟用	啟用	啟用

Network Security:Do not store LAN Manager hash value on next password change (網路安全性：當下次密碼更改時，不要儲存 LAN Manager 雜湊值) 安全性選項設定值可決定當密碼更改時，是否要儲存新密碼的 LAN Manager (LM) 雜湊值。LM 的雜湊法十分脆弱且易於受攻擊，相較之下 Windows NT 的雜湊密碼比較強。因此，本手冊所定義的安全性環境都將此選項設成啟用(Enabled)。

注意：當此設定啟用時，極舊版的作業系統和某些協力廠商的應用程式可能會失敗。此外，當您啓用此設定之後，可能需要變更所有帳戶的密碼。

網路安全性：LAN Manager 驗證層級

表 3.96：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
僅傳送 NTLM 回應	僅傳送 NTLMv2 回應	僅傳送 NTLMv2 回應\拒絕 LM	僅傳送 NTLMv2 回應\拒絕 LM & NTLM

Network Security：LAN Manager authentication level (網路安全性：LAN Manager 驗證層級) 安全性選項設定值可決定哪個挑戰/回應驗證通訊協定可用於網路登入中。此選擇將影響用戶端所使用的驗證通訊協定層級、交涉的安全性層級、伺服器接受的驗證層級，如下所示。底下的括弧內數字代表「LMCompatibilityLevel」登錄值的實際設定。您應根據下列方針，將此選項設成您系統環境所能容許的最高層級：

對於單純的 Windows NT 4.0 SP4 或以後版本的環境 – 包括 Windows 2000 和 Windows XP Professional – 在所有的用戶端上將此選項設成「Send NTLMv2 response only/refuse LM & NTLM」，並在所有的用戶端設好之後，在所有的伺服器上將它設成「Send NTLMv2 response only/refuse LM & NTLM」。此建議值的例外是 Windows 2003 Routing and Remote Access (Windows 2003 路由及遠端存取) 伺服器，若您將此選項設得高於「Send NTLMv2 response only/refuse LM」，此伺服器將無法正常運作。

企業用戶端環境包含了 Routing and Remote Access 伺服器。基於此理由，此環境會將此選項設成「Send NTLMv2 response only/refuse LM」。高安全性環境並未包含 Routing and Remote Access 伺服器，因此這個環境會將該選項設成「Send NTLMv2 response only/refuse LM & NTLM」。

若您擁有 Windows 9x 用戶端，並可將 DSClient 安裝到這所有的用戶端上，請在執行 Windows NT (Windows NT、Windows 2000 和 Windows XP Professional) 的電腦上將此選項設成「Send NTLMv2 response only/refuse LM & NTLM」。否則，在非執行 Windows 9x 的電腦上，此選項的設定值不得高於「Send NTLMv2 responses only」。

若您發現啓用此設定會令某些應用程式中斷，可一次復原一個步驟，來找出中斷的項目。您至少應在所有電腦上都將此選項設成「Send LM & NTLM - use NTLMv2 session security if negotiated」，一般而言，我們可將系統環境中的所有電腦上設成「Send NTLMv2 responses only」。

網路安全性：LDAP 用戶端簽章需求

表 3.97：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
交涉簽章	交涉簽章	交涉簽章	交涉簽章

Network Security:LDAP client signing requirements (網路安全性：LDAP 用戶端簽章需求) 安全性選項設定值可決定要代表發出 LDAP BIND 要求之用戶端所需的資料簽章層級。未簽章的網路傳輸極易受到中間人攻擊。在 LDAP 伺服器的狀況中，這意味著駭客可能會讓伺服器根據來自 LDAP 用戶端的錯誤查詢來做決定。因此，本手冊所定義的三個系統環境都將此選項設成「Negotiate signing」。

網路安全性：NTLM SSP 型 (包括安全的 RPC) 用戶端的最小工作階段安全性

表 3.98：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
無最小值	無最小值	啓用所有設定值	啓用所有設定值

Network Security:Minimum session security for NTLM SSP based (including secure RPC) clients (網路安全性：NTLM SSP 型 (包括安全的 RPC) 用戶端的最小工作階段安全性) 安全性選項設定值可讓用戶端要求交涉訊息機密性 (加密)、訊息簽章、128-bit 加密或 NTLM 2 版 (NTLMv2) 工作階段安全性。此選項的設定值越高越好，並讓網路上的應用程式能夠充分運作，以確保來自 NTLM SSP 伺服器的網路傳輸不會受到中間人攻擊，資料也不會曝光。

網路安全性：NTLM SSP 型 (包括安全的 RPC) 伺服器的最小工作階段安全性

表 3.99：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
無最小值	無最小值	啓用所有設定值	啓用所有設定值

Network Security:Minimum session security for NTLM SSP based (including secure RPC) servers (網路安全性：NTLM SSP 型 (包括安全的 RPC) 伺服器的最小工作階段安全性) 安全性選項設定值可讓伺服器要求交涉訊息機密性 (加密)、訊息完整性、128-bit 加密或 NTLMv2 工作階段安全性。請將此選項設得越高越好，並讓網路上的應用程式能夠充分運作，以確保來自 NTLM SSP 用戶端的網路傳輸不會受到中間人攻擊，資料也不會曝光。

復原主控台：允許自動管理登入

表 3.100：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	停用	停用

Recovery console:Allow automatic administrative logon (復原主控台：允許自動管理登入) 安全性選項設定值可決定是否必須先提供「Administrator」帳戶的密碼，方能存取系統。若將此選項設成啟用，復原主控台並不會要求您提供密碼，而且它會自動登入到系統內。當疑難排解和修復系統無法正常地重新啟動時，復原主控台將會非常有用。不過，啟用此設定可能很危險，因為之後任何人都可到伺服器旁切斷電源將它關機、重新啟動它、選取「Restart」功能表中的「Recover Console」，接著完全控制伺服器。因此，本手冊所定義的三個系統環境都將此選項設成預設值。若要在此選項設成停用時使用復原主控台，使用者必須輸入使用者名稱和密碼，方能存取復原主控台的帳戶。

復原主控台：允許磁片複製與存取所有磁碟機和所有資料夾

表 3.101：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	啟用	啟用	停用

啟用 Recovery console:Allow floppy copy and access to all drives and all folders (復原主控台：允許磁片複製與存取所有磁碟機和所有資料夾) 安全性選項設定值可讓復原主控台的 SET 指令供您使用，如此您就可設定下列的復原主控台環境變數：

- AllowWildCards:替一些指令提供萬用字元支援 (例如 DEL 指令)。
- AllowAllPaths:允許存取電腦上的所有檔案和資料夾。
- AllowRemovableMedia:允許將檔案複製到抽取式媒體，例如磁片。
- NoCopyPrompt:在覆寫現有檔案時不顯示提示。

為取得最大的安全性，高安全性環境會將此選項設成「停用(Disabled)」。

關機：允許系統不用登入即可關機

表 3.102：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	停用	停用

Shutdown:Allow system to be shut down without having to log on (關機：允許系統不用登入即可關機) 安全性選項設定值可決定電腦可否不用登入到 Windows 作業系統內即可關機。此意味能夠可存取主控台的使用者便可將系統關機。駭客或誤導的使用者可透過終端機服務連至伺服器，並將它關機，或不需識別自身即重新啟動它。因此，在三個系統環境中都應將此反制措施設成預設值。

關機：清除虛擬記憶體分頁檔

表 3.103：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	停用	啟用

Shutdown:Clear virtual memory page file (關機：清除虛擬記憶體分頁檔) 安全性選項設定值可決定虛擬記憶體分頁檔是否在系統關機時清除。當此設定啟用時，每次系統成功地關機時，系統都會清除系統分頁檔。若您啟用此安全性設定時，且可攜式電腦系統設定成休眠停用時，休眠檔(hiberfil.sys)便會全部填入零值。將伺服器關機和重新啟動所需的時間會比較長，若伺服器包含較大的分頁檔，此時間更是明顯。基於這些理由，高安全性環境會將此選項設成啟用(Enabled)，而舊版用戶端和企業用戶端環境則將它設成停用(Disabled)。

注意：能夠實體存取伺服器的駭客只要拔掉伺服器的電源，即可避開此反制措施。

系統加密：替儲存於電腦上的使用者金鑰強制運用強式金鑰保護

表 3.104：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
未定義	第一次使用金鑰時提示使用者	第一次使用金鑰時提示使用者	每次使用者使用金鑰時都必須輸入密碼

System cryptography:Force strong key protection for user keys stored on the computer (系統加密：替儲存於電腦上的使用者金鑰強制運用強式金鑰保護) 安全性選項設定值可決定使用者的私密金鑰(例如其 S-MIME 金鑰) 需要有密碼方能使用。若您將此原則設成每次使用者使用金鑰時，都必須提供不同於網域密碼的密碼，那麼即使駭客控制其電腦，並發現其登入密碼，要存取存在本機的使用者金鑰仍然極為困難。在舊版用戶端和企業用戶端環境中，請將此選項的值設成「User is prompted when the key is first used (第一次使用金鑰時提示使用者)」設定選項。

為了進一步地確保系統環境安全性，高安全性環境應此選項設成「User must enter a password each time they use a key (每次使用者使用金鑰時都必須輸入密碼)」。

系統加密：使用 FIPS 相容演算法來進行加密、雜湊和簽章

表 3.105：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	停用	停用

System cryptography:Use FIPS compliant algorithms for encryption, hashing, and signing (系統加密：使用 FIPS 相容演算法來進行加密、雜湊和簽章) 安全性選項設定值可決定 Transport Layer Security/Secure Sockets Layer (TLS/SSL) 的安全性提供者 (Security Provider) 是否只支援 TLS_RSA_WITH_3DES_EDE_CBC_SHA 密碼套件。啓用此原則可確保您系統環境中的電腦將會使用最強大的演算法來進行數位加密、雜湊和簽章。這可盡量降低未經授權的使用者破壞數位加密或簽章資料的風險。基於這些理由，本手冊所定義的三個系統環境都將此選項設成停用(Disabled)。

系統物件：Administrators 群組之成員所建立物件的預設擁有者

表 3.106：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
管理員群組	物件建立者	物件建立者	物件建立者

System objects:Default owner for objects created by members of the Administrators group (系統物件：Administrators 群組之成員所建立物件的預設擁有者) 安全性選項設定值可決定 Administrators 群組或物件建立者是否能夠成爲所建立的任何系統物件的預設擁有者。當系統物件建立時，擁有權會指出哪個帳戶建立該物件，而非較籠統的 Administrators 群組。

系統物件：非 Windows 子系統需要不區分大小寫

表 3.107：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
啓用	啓用	啓用	啓用

System objects:Require case insensitivity for non-Windows subsystems (系統物件：非 Windows 子系統需要不區分大小寫) 安全性選項設定值可決定是否所有子系統都強制運用不區分大小寫。Microsoft Win32 的子系統並不會區分大小寫。不過，核心仍可支援其他子系統的區分大小寫，例如 Portable Operating System Interface for UNIX (POSIX)。因爲 Windows 並不會區分大小寫 (但是 POSIX 子系統將支援區分大小寫)，若不強制運用此設定，則子系統的使用者可透過大小寫混雜的檔名，建立一個和另一個檔案同名的檔案。如此做將會阻止另一個使用者以正常的 Win32 工具存取這些檔案，因爲只有一個檔案可供使用。爲確保檔案名稱的一致性，本手冊所定義的三個系統環境都將此設定設成啓用(Enabled)。

系統物件：加強內部系統物件 (例如符號連結) 的預設權限

表 3.108：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
啟用	啟用	啟用	啟用

System objects:Strengthen default permissions of internal system objects (e.g. Symbolic Links) (系統物件：加強內部系統物件 (例如符號連結) 的預設權限) 安全性選項設定值可決定物件的預設判別存取控制清單 (DACL) 的強度。此選項有助於保護可能位於、共用於不同處理序的物件。將此選項設成預設值可強化 DACL，讓並非管理員的使用者可讀取共用的物件，但無法修改任何不是他們所建立的物件。因此，本手冊所定義的三個系統環境都將此選項設成停用(Enabled)的預設值。

系統設定：選擇性子系統

表 3.109：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
POSIX	無	無	無

System settings:Optional subsystems (系統設定：選擇性子系統) 安全性選項設定值可決定哪些子系統可用來支援您系統環境中的應用程式。在 Windows Server 2003 中，此設定的預設值為 POSIX。為了停用 POSIX 子系統，本手冊所定義的三個系統環境都將此選項設成「None」。

事件記錄檔

事件記錄檔記錄了系統中的各種事件。安全性記錄檔則記錄稽核事件。群組原則的事件記錄檔容器可用來定義應用程式、安全性和系統事件記錄檔的相關屬性，例如最大的記錄檔大小、每個記錄檔的存取權限、保存設定和方法的相關屬性。應用程式、安全性和系統事件記錄檔的設定值都設定於 MSBP 內，並套用到網域內的所有成員伺服器上。在 Windows Server 2003 中，事件記錄檔設定可在「群組原則物件編輯器」的下列位置中設定：

Computer Configuration\Windows Settings\Security Settings\Event Log

本節詳述了在 MSBP 中，本手冊所定義三個系統環境的預設安全性選項。如需本節所預定的設定摘要，請參閱「Windows Server 2003 Security Guide Settings Excel」工作簿。如需預設設定的相關資訊，及此節所討論的每個設定的詳細說明資訊，請參閱所附手冊《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》，網址為：<http://go.microsoft.com/fwlink/?LinkId=15159>。

最大的應用程式記錄檔容量

表 3.110：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
16,384 KB	16,384 KB	16,384 KB	16,384 KB

Maximum application log size (最大的應用程式記錄檔大小) 安全性設定可決定應用程式事件記錄檔的最大容量，其最大容量為 4 (GB)，不過這並非建議值，因為記憶體分割的風險會導致效能降低與事件記錄不可靠。應用程式記錄檔的大小需求將取決於平台的功能，以及應用程式相關事件的歷史記錄需求。本手冊所定義的三個系統環境都採用預設值 16,384 (KB)。

最大的安全性記錄檔容量

表 3.111：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
16,384 KB	81,920 KB	81,920 KB	81,920 KB

Maximum security log size (最大的安全性記錄檔容量) 安全性設定值可指定安全性事件記錄檔的最大容量，其最大容量為 4 GB。在網域控制站和獨立的伺服器上，至少要將安全性記錄檔設成 80 MB，如此才能夠儲存足夠的資訊去進行稽核。要將其他系統的記錄檔容量設定到一定足夠的程度時，您必須考量記錄檔的檢視頻率、可用的磁碟空間等因素。

最大的系統記錄檔容量

表 3.112：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
16,384 KB	16,384 KB	16,384 KB	16,384 KB

Maximum system log size (最大的系統記錄檔容量) 安全性設定值可指定應用程式事件記錄檔的最大容量，其最大容量為 4 (GB)，不過這並非建議值，因為記憶體分割的風險會導致效能降低與不可靠的事件記錄。應用程式記錄檔容量的需求是取決於平台的功能，以及應用程式相關事件的歷史記錄需求。本手冊所定義的三個系統環境都採用預設值 16,384 KB。

防止本機訪客群組存取應用程式記錄檔

表 3.113：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
啟用	啟用	啟用	啟用

Prevent local guests group from accessing application log (防止本機訪客群組存取應用程式記錄檔) 此安全性設定值可決定是否要禁止訪客存取應用程式事件記錄檔。在預設狀態下，Windows Server 2003 的所有系統都不允許訪客進行存取。因此，此設定在預設系統中並沒有任何實質效果。不過，它可視為一個沒有副作用的防禦性設定。

注意：此設定並未出現在 Local Computer Policy (本機電腦原則) 物件中。

防止本機訪客群組存取安全性記錄檔

表 3.114：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
啟用	啟用	啟用	啟用

Prevent local guests group from accessing security log (防止本機訪客群組存取安全性記錄檔) 此安全性設定值可決定是否要禁止訪客存取安全性事件記錄檔。使用者必須擁有 Manage (管理) 稽核和安全性記錄檔的使用者權限 (未定義於本手冊內)，方能存取安全性記錄檔。因此，此設定在預設系統上並沒有任何實質效果。不過，它可視為一個沒有副作用的防禦性設定。

注意：此設定並未出現在 Local Computer Policy (本機電腦原則) 物件中。

防止本機訪客群組存取系統記錄檔

表 3.115：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
啟用	啟用	啟用	啟用

Prevent local guests group from accessing system log (防止本機訪客群組存取系統記錄檔) 此安全性設定值可決定是否要禁止訪客存取系統事件記錄檔。在預設狀態下，Windows Server 2003 的所有系統都不允許訪客進行存取。因此，此設定在預設系統中並沒有任何實質效果。不過，它可視為一個沒有副作用的防禦性設定。

注意：此設定並未出現在 Local Computer Policy (本機電腦原則) 物件中。

應用程式記錄檔的保存方法

表 3.116：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
依需要	依需要	依需要	依需要

Retention method for application log (應用程式記錄檔的保存方法) 此安全性設定值可決定應用程式記錄檔的“打包”方法。若基於法律或疑難排解的用途，需要用到歷史性事件，您務必經常保存應用程式記錄檔。請依需要覆寫事件，以確保記錄檔一直儲存最近的事件，不過這可能會損失歷史性資料。

安全性記錄檔的保存方法

表 3.117：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
依需要	依需要	依需要	依需要

Retention method for security log (安全性記錄檔的保存方法) 此安全性設定值可決定安全性記錄檔的“打包”方法。若基於法律或疑難排解的用途，需要用到歷史性事件，您務必經常保存安全性記錄檔。請依需要去覆寫事件以確保記錄檔一直儲存最近的事件，不過這可能會造成歷史性資料的損失。

系統記錄檔的保存方法

表 3.118：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
依需要	依需要	依需要	依需要

Retention method for system log (系統記錄檔的保存方法) 此一安全性設定值可決定系統記錄檔的“打包”方法。若基於法律或疑難排解的用途，需要用到歷史性事件，您務必經常保存該記錄檔。請依需要去覆寫事件以確保記錄檔一直儲存最近的事件，不過這可能會造成歷史性資料的損失。

系統服務

當 Windows Server 2003 第一次安裝時，將會建立預設的系統服務，並將它們設成系統一啓動便執行。這些系統服務中有許多並不需要在本手冊所定義的三個系統環境中執行。Windows Server 2003 提供了一些額外的選擇性服務，例如 Certificate Services (認證服務)，它們並未安裝於 Windows Server 2003 的預設安裝之中。要將這些選擇性服務加入現有的系統內，您可使用「Add/Remove Programs」或「Windows Server 2003 Configure Your Server Wizard」，或建立可自訂的 Windows Server 2003 自動化安裝。

任何服務或應用程式都是潛在的攻擊點。因此，目標環境中任何不需要的服務或執行檔都應停用或移除。MSBP 只會讓 Windows Server 2003 成員伺服器所需的服務納入 Windows Server 2003 網域內，以提供基本的管理服務。而每個伺服器所需的特定服務也都將啓用。特定的群組原則將在本手冊的其他章節做描述，那裡會詳細地描述強化每個伺服器角色所需的特定步驟。

每個伺服器角色所需的特定服務，將以每一伺服器為基礎去啓用 — 這些伺服器角色的特定群組原則將於底下的章節中描述。若本手冊所定義的系統環境中需要附加的伺服器角色，那您可能需要替它們啓用附加的服務。例如，若想以 Microsoft SQL Server 在 Web 應用程式後端儲存客戶的資料，那您就需要安裝 SQL Server。在此狀況中，您將需要建立套用至該新伺服器角色的群組原則，將 SQL Services 服務設成自動(Automatic)。

注意：若啓用附加的服務，它們可能又需要進一步的服務。特定伺服器角色所需的所有服務，都會加到該伺服器在您組織中所執行伺服器角色的原則內。

在 Windows Server 2003 中，系統服務設定可以在「群組原則物件編輯器」的下列位置中設定：

Computer Configuration\Windows Settings\Security Settings\System Services\

本節詳述了針對 MSBP，本手冊所定義三個系統環境的預定安全性選項。如需本章節所預定設定的摘要，

請參閱「Windows Server 2003 Security Guide Settings Excel」工作簿。如需預設設定的相關資訊，及此節所討論的每個設定的詳細說明資訊，請參閱所附手冊《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》，網址為：<http://go.microsoft.com/fwlink/?LinkId=15159>。

警示器

表 3.119：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Alerter	停用	停用	停用	停用

Alerter(警示器) 系統服務會將管理警示通知所選定的使用者和電腦。使用 Alerter 服務來傳送警示訊息給連至您網路的指定使用者。為確保本手冊所定義的三個系統環境擁有更大的安全性，請停用此服務。若停止此服務，使用管理警示的程式將不會收到它們。

注意：停用此服務，可能會破壞不斷電供電 (UPS) 警示訊息系統的功能。

應用程式層閘道服務

表 3.120：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
ALG	手動	停用	停用	停用

Application Layer Gateway Service (應用程式層閘道服務) 系統服務是 Internet Connection Sharing (網際網路連線共用，簡寫為 ICS) / Internet Connection Firewall (網際網路連線防火牆，簡寫為 ICF) 服務的子元件，它可支援獨立軟體廠商 (ISV) 編寫通訊協定外掛模組，讓其專用的網路通訊協定通過防火牆，並運作於 ICS 後面。為確保本手冊所定義的三個系統環境擁有更大的安全性，並防止未授權的電腦被利用作為 Internet 閘道，請停用此系統服務。

應用程式管理

表 3.121：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
AppMgmt	手動	停用	停用	停用

Application Management (應用程式管理) 系統服務提供了軟體安裝服務，例如 Assign、Publish 和 Remove。此服務處理序要求列舉、安裝和移除經由共同網路部署的程式。當您連結至網域的電腦上，並按了「Add/Remove Programs」之後，程式將會呼叫此服務去取得所部署程式的清單。大多數的公司並不會在伺服器上使用此系統服務；反之，它們都使用自動化的軟體供應應用程式來散發軟體套件。基於這些理由，請在基礎伺服器原則上停用此服務。

ASP.NET 狀態服務

表 3.122：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
aspnet_state	未安裝	停用	停用	停用

ASP.NET State Service (ASP.NET 狀態服務) 系統服務支援 ASP.NET 的跨處理序 (Out-Of-Process) 工作階段狀態。在基礎原則中，此服務將設成停用(Disabled)。

自動更新

表 3.123：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
wuauerv	自動	自動	自動	自動

Automatic Updates (自動更新) 系統服務可讓您下載與安裝重要的 Windows 更新項目。為確保本手冊所定義的三個系統環境擁有更大的安全性，請停用此服務。若要搜尋、下載和安裝可套用的重要修復項目，請造訪 Windows 更新網站 <http://v4.windowsupdate.microsoft.com/en/default.asp>。

背景智慧型傳輸服務，簡寫為 BITS

表 3.124：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
BITS	手動 - 若 BITS 工作暫止 的話則為自動	手動	手動	手動

Background Intelligent Transfer Service (背景智慧型傳輸服務，簡寫為 BITS) 系統服務是一個背景檔傳輸機制和佇列管理員。BITS 可以非同步地在用戶端和 HTTP 伺服器之間傳送檔案。BITS 服務將接受要求，以閒置的網路頻寬來傳送檔案，因此其他的網路相關活動，例如瀏覽，並不會受到影響。本手冊所定義的三個系統環境都將此選項設成「Manual(手動)」。

認證服務

表 3.125：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
CertSvc	未安裝	停用	停用	停用

Certificate Services (認證服務) 系統服務是核心作業系統的一部份，它可讓某個企業作為自己的認證授權 (CA)，並發出與管理數位認證。此服務僅適合特定的伺服器角色。因此，在本手冊所定義三個系統環境的基礎伺服器原則中，請停用此設定。

MS 軟體陰影複本提供者

表 3.165：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
SwPrv	手動	手動	手動	手動

MS Software Shadow Copy Provider (MS 軟體陰影複本提供者) 系統服務可管理檔案陰影複本的軟體，Volume Shadow Copy 服務將會用到這些複本。陰影複本可讓您建立磁碟區的複本 (或明顯複本)，以代表該磁碟區一致的唯讀時點資料。之後，此時點的資料將維持不變，並可讓 Ntbackup 之類的應用程式從陰影複本中將資料複製到磁帶上。若停用此服務，就無法管理軟體型態的磁碟區陰影複本。

Netware 的用戶端服務

表 3.126：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
NWCWorkstation	未安裝	停用	停用	停用

Client Service for Netware (Netware 的用戶端服務) 系統服務可讓以互動方式登入至服務所在伺服器上的使用者存取 NetWare 網路上的檔案與列印資源。透過 Client Service for Netware，您可從您的電腦中存取執行 Novell Directory Services (NDS) 或連結安全性 (NetWare 3.x 或 4.x 版) 之 Netware Servers 上的檔案與列印資源。為確保本手冊所定義的三個系統環境擁有更大的安全性，請停用此服務。

剪貼本

表 3.127：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
ClipSrv	停用	停用	停用	停用

ClipBook(剪貼本) 系統服務可讓 Clipbook Viewer 建立與共用資料“分頁”，並透過遠端電腦來檢視。此服務將倚賴 Network Dynamic Data Exchange (NetDDE) 服務來建立其他電腦可連接的實際檔案共用區，而 Clipbook 應用程式和服務可讓您建立欲共用的資料分頁。

為確保本手冊所定義的三個系統環境擁有更大的安全性，請停用此服務。任何明確倚賴此服務的服務將無法啟動。Clipbrd.exe 仍可用來檢視本機的剪貼簿 – 也就是當使用者選取文字，接著按編輯(Edit)功能表上的複製(Copy)，或按 CTRL+C 之後，資料所存放的位置。

叢集服務

表 3.128：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
ClusSvc	未安裝	停用	停用	停用

Cluster Service (叢集服務) 系統服務可控制伺服器叢集作業與管理叢集資料庫。叢集是獨立電腦的集合，它用起來就和使用單一電腦一樣簡單，但在管理上可能極為困難。管理員將它視為單一系統，而程式設計師和使用者亦將之視為單一系統。Cluster Service 會將資料和運算分配給叢集的不同節點。當某個節點失敗時，其他節點將提供該遺失節點先前所提供的服務和資料。當節點加入或修復時，Cluster Service 軟體會將一些資料和運算轉移到該節點上。為確保本手冊所定義的三個系統環境擁有更大的安全性，請停用此服務。

COM+ 事件系統

表 3.129：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
COMSysApp	手動	手動	手動	手動

COM+ Event System (COM+ 事件系統) 服務會自動散發事件給訂閱 COM 元件。COM+ Events 服務會擴充 COM+ 程式設計模型，以支援晚期繫結事件或發行者或訂閱者和事件系統之間的方法呼叫。現在您不需重複地輪詢伺服器，因為事件系統將在資訊可供使用時通知您。為提供使用性和更大的安全性給本手冊所定義的三個系統環境，請將此服務設成「Manual(手動)」。

COM+ 系統應用程式

表 3.130：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
EventSystem	手動	停用	停用	停用

COM+ System Application (COM+ 系統應用程式) 系統服務可管理 COM+ 型元件的組態設定與追蹤。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用 (Disabled)。

電腦瀏覽器

表 3.131：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
瀏覽器	自動	自動	自動	自動

Computer Browser (電腦瀏覽器) 服務會維護您網路上最新的電腦清單，並提供此清單給要求它的程式。Computer Browser 服務將由需要檢視網路網域和資源的 Windows 型態電腦所使用。為確保本手冊所定義的三個系統環境擁有更大的安全性，請將此服務設成「Automatic(自動)」。

加密服務

表 3.132：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
CryptSvc	自動	自動	自動	自動

Cryptographic Services (加密服務) 系統服務可替您的電腦提供金鑰管理服務。為確保本手冊所定義的三個系統環境擁有更大的安全性，此系統服務會將此服務設成「Automatic(自動)」。若停止此服務，以上所述的管理服務將無法正常運作。

DHCP 用戶端

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Dhcp	自動	自動	自動	自動

DHCP Client (DHCP 用戶端) 系統服務可管理網路組態，其作法是註冊與更新 IP 位址，並以 DNS 伺服器更新您電腦的 Dynamic Domain Naming Service (DDNS) 項目。當用戶端 (例如漫遊使用者) 在網路內閒逛時，您並不需要手動地變更 IP 設定。不管用戶端重新連接到哪個子網路，該用戶端都會自動被賦予一個新的 IP 位址 – 只要它可從這每一個子網路中存取得到 DHCP 伺服器即可。為確保本手冊所定義的三個系統環境擁有更大的安全性，請將此選項設成「Automatic(自動)」。若停止此服務，您的電腦將不會收到動態的 IP 位址和 DNS 更新項目。此外也要注意，停用 DHCP 用戶端將會令伺服器無法透過 DDNS 來註冊於 DNS。

DHCP 伺服器

表 3.134：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
DHCP Server	未安裝	停用	停用	停用

DHCP Server (DHCP 伺服器) 系統服務會自動配置 IP 位址，並啟用進階的網路設定組態 (例如 DNS 伺服器和 WINS 伺服器) 給 DHCP 用戶端。本手冊所定義三個系統環境中的成員伺服器並不需要 DHCP Server 服務。不過，對於三個系統環境中的 DHCP 伺服器而言，則需要此設定，請將其設成「Automatic(自動)」。

分散式檔案系統

表 3.135：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Dfs	自動	停用	停用	停用

Distributed File System (分散式檔案系統，簡寫為 DFS) 服務可管理分散於本機或廣域網路上的邏輯磁碟區。DFS 是一個分散式服務，可將不同的檔案共用區整合到單一的邏輯命名空間內。本手冊所定義三個系統環境中的成員伺服器並不需要 DFS。不過，對於三個系統環境中的網域控制站而言，則需要此設定，並將之設成「Automatic(自動)」。

分散式連結追蹤用戶端

表 3.136：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
TrkWks	自動	停用	停用	停用

Distributed Link Tracking Client (分散式連結追蹤用戶端) 系統服務可維護您電腦內的 NTFS 檔之間的連結或您網路網域內不同電腦間的連結。Distributed Link Tracking (DLT) Client 服務可確保捷徑和物件連結與內嵌 (OLE) 連結可在目標檔案重新命名或移動之後持續運作。為確保本手冊所定義的三個系統環境擁有最大的安全性，請停用「Distributed Link Tracking Client」服務。若停止此服務，您電腦上的連結將無法維護或追蹤。

分散式連結追蹤伺服器

表 3.137：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
TrkSvr	手動	停用	停用	停用

Distributed Link Tracking Server (分散式連結追蹤伺服器) 系統服務可儲存資訊，讓網域內每個磁碟區都可追蹤移動於磁碟區之間的檔案。若此選項設成啟用，Distributed Link Tracking Server 服務將在網域控制站上執行。因此，網域控制站的原則只會將此服務設成「Automatic(自動)」。

分散式交易協調器

表 3.138：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
MSDTC	自動	停用	停用	停用

Distributed Transaction Coordinator (分散式交易協調器) 系統服務負責協調分散於多個電腦系統或資源管理員 (例如資料庫、訊息佇列、檔案系統或其他的交易保護資源管理員) 的交易。本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

DNS 用戶端

表 3.139：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Dnscache	自動	自動	自動	自動

DNS Client (DNS 用戶端) 系統服務會替您的電腦解析與快取 DNS 名稱。DNS 用戶端服務必須執行於每台執行 DNS 名稱解析的電腦上。解析 DNS 名稱對於在 Active Directory 網域中尋找網域控制站相當重要。執行 DNS 用戶端服務對於尋找以 DNS 名稱解析來識別身份的裝置也很重要。基於這些理由，本手冊所定義的三個系統環境都將此服務設成「Automatic(自動)」。

DNS 伺服器

表 3.140：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
DNS	未安裝	停用	停用	停用

DNS Server (DNS 伺服器) 系統服務透過回覆有關 DNS 名稱的查詢和更新要求，啟用 DNS 名稱解析。擁有 DNS 伺服器對於尋找以 DNS 名稱和網域控制站來識別身份的裝置非常重要。基礎伺服器並不需要這些功能；只有在網域控制站上才需用到它們。因此，本手冊所定義三個系統環境的基礎原則都將此選項設成停用。只有在三個系統環境的 DNS 伺服器上才將此系統服務的值設成「Automatic(自動)」。

錯誤報告服務

表 3.141：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
ERSvc	自動	停用	停用	停用

Error Reporting Service (錯誤報告服務) 系統服務會收集、儲存和報告未預期的應用程式關閉給 Microsoft，並替執行於非標準環境內的服務和應用程式授權錯誤報告。此服務提供高效率的有效資訊給 Microsoft 產品群組，以偵錯驅動程式和應用程式的錯誤。若啟用 Display Error Notification 服務，使用者仍會收到一個發生問題的警示訊息，但他們並無法將此資訊報給 Microsoft 或本機網路錯誤報告伺服器。基於這些理由，本手冊所定義的三個系統環境都將此服務設成停用。

事件記錄檔

表 3.142：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Eventlog	自動	自動	自動	自動

Event Log (事件記錄檔) 系統服務可讓 Windows 型態的程式和元件所發出的事件記錄檔訊息可檢視於事件檢視器上。事件記錄檔報告中包含了可用來診斷問題的資訊。若 Event Log 停用，您將無法追蹤事件，這將會大幅降低成功診斷系統問題的能力。因此，本手冊所定義的三個系統環境都將此服務設成「Automatic(自動)」。

傳真服務

表 3.143：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
傳真	未安裝	停用	停用	停用

Fax Service (傳真服務) 系統服務是一個 Telephony API (TAPI) 的相容服務，可透過您的電腦提供傳真能力。Fax Service 可讓使用者透過本機的傳真裝置或共用的網路傳真裝置，從其桌面應用程式傳送與接收傳真。在基礎伺服器上，此服務是設定成停用，因此您的電腦無法傳送或接收傳真。

檔案複寫

表 3.144：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
NtFrs	手動	停用	停用	停用

File Replication Service (檔案複寫服務，簡寫為 FRS) 可讓檔案同時自動地複製與維護於多重伺服器上。若 File Replication Service 為停用，檔案複寫將不會發生，而伺服器資料也不會同步化。就網域控制站而言，停止 FRS 服務可能會大幅降低網域控制站正常運作的能力。因此，雖然基礎原則將此服務的値設成停用(Disabled)。不過，本手冊所定義三個系統環境的網域控制站基礎原則都將此選項設成「Automatic(自動)」。

Macintosh 的檔案伺服器

表 3.145：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
MacFile	未安裝	停用	停用	停用

File Server for Macintosh (Macintosh 的檔案伺服器) 系統服務可讓 Macintosh 使用者儲存與存取本機 Windows 伺服器電腦上的檔案。這並非標準伺服器環境的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用 (Disabled)。

FTP 發行服務

表 3.146：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
MSFtpsvc	未安裝	停用	停用	停用

FTP Publishing Service (FTP 發行服務) 透過 IIS 嵌入式管理單元提供連接和管理能力。FTP Publishing Service 並非標準伺服器環境的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用 (Disabled)。

說明及支援

表 3.147：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Helpsvc	自動	停用	停用	停用

Help and Support (說明及支援) 系統服務可讓「說明及支援中心」(Help and Support Center) 在您的電腦上執行。此服務支援「說明及支援中心」應用程式，並讓用戶端應用程式和說明資料彼此通訊。若停用此系統服務，「說明及支援中心」將無法使用。本手冊所定義的三個系統環境都將此服務設成停用 (Disabled)。

HTTP SSL

表 3.148：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
HTTPFilter	手動	停用	停用	停用

HTTP SSL 系統服務可讓 IIS 執行 SSL 功能。HTTP SSL 服務可啓用安全的電子交易；不過，爲了減少攻擊漏洞，建議您在基礎原則中將此服務設成停用 (Disabled)。在 IIS 伺服器角色原則中，只應將此服務設成「Automatic(自動)」。

人性化介面裝置存取

表 3.149：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
HidServ	停用	停用	停用	停用

Human Interface Device Access (人性化介面裝置存取) 系統服務提供泛用的輸入存取給 Human Interface Devices (人性化介面裝置，簡寫爲 HID)，以啓用和維護鍵盤、遙控器和其他多媒體裝置上的預定快速按鈕的使用。基礎伺服器環境並不需要這些功能。基於此理由，請將此服務的值設成停用 (Disabled)。

IAS Jet 資料庫存取

表 3.150：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
IASJet	未安裝	停用	停用	停用

IAS Jet Database Access (IAS Jet 資料庫存取) 系統服務只能用於 Windows Server 2003 的 64-bit 版本。此服務使用 Remote Authentication Dial-in User Service (RADIUS) 通訊協定來提供驗證、授權和帳戶服務。此服務設成停用(Disabled)。

IIS 管理服務

表 3.151：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
IISADMIN	未安裝	停用	停用	停用

IIS Admin Service (IIS 管理服務) 可讓您管理 IIS 元件，例如 FTP、應用程式集區、網站、Web 服務擴充功能和 Network News Transfer Protocol (網路新聞傳輸通訊協定，簡寫為 NNTP) 與 Simple Mail Transfer Protocol (簡單郵件傳輸通訊協定，簡寫為 SMTP) 虛擬伺服器。若此服務停用，您將無法執行 Web、FTP、NNTP 或 SMTP 網站。基於此理由，請在 IIS 伺服器原則內將此服務設成「Automatic(自動)」。基礎伺服器環境並不需要這些功能。因此，此服務將設成停用(Disabled)。不過，IIS 角色原則將此服務設成「Automatic(自動)」。

IMAPI CD-Burning COM Service

表 3.152：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
ImapiService	停用	停用	停用	停用

IMAPI CD-Burning COM Service (IMAPI CD-燒錄 COM 服務) 可透過 Image Mastering Applications Programming Interface (IMAPI) COM 介面來管理 CD 燒錄，並當使用者透過 Windows 檔案總管、Windows Media Player (WMP) 或使用此 API 的協力廠商應用程式來要求時，執行 CD-R 寫入。基礎伺服器環境並不需要這些功能。因此，此服務設成停用(Disabled)。

索引服務

表 3.153：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Cisvc	停用	停用	停用	停用

Indexing Service (索引服務) 會替本機和遠端電腦上的檔案內容和屬性建立索引，並透過彈性的查詢語言，讓使用者快速地存取檔案。Indexing Service 也可讓您快速地搜尋本機和遠端電腦上的文件，並替共享於 Web 上的內容提供搜尋索引。基礎伺服器環境並不需要這些功能。因此，此服務將設成停用(Disabled)。

紅外線監視器

表 3.154：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Irmon	未安裝	停用	停用	停用

Infrared Monitor (紅外線監視器) 系統服務可讓您使用紅外線來共用檔案和影像。在預設狀態下，只要是在安裝 Windows Server 2003 作業系統時偵測得到紅外線裝置，系統就會安裝此服務。此服務並無法用於 Windows Server 2003 Web、Enterprise 或 Datacenter Server 上。

若此服務停用，檔案和影像都無法使用紅外線來共用。基礎伺服器環境並不需要這些功能。因此，將此服務將設成停用(Disabled)。

網際網路驗證服務

表 3.155：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
IAS	未安裝	停用	停用	停用

Internet Authentication Service (網際網路驗證服務，簡寫為 IAS) 可以集中管理網路存取驗證、授權、稽核和帳戶。IAS 適用於虛擬私人網路 (VPN)、撥號、802.1X 無線或 IETF RADIUS 通訊協定的相容存取伺服器所傳送的 Ethernet 交換連線嘗試。基礎伺服器環境並不需要這些功能。因此，此服務將設成停用(Disabled)。

網際網路連線防火牆

表 3.156：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
SharedAccess	停用	停用	停用	停用

Internet Connection Firewall (網際網路連線防火牆，簡寫為 ICF)/Internet Connection Sharing (網際網路連線共用，簡寫為 ICS) 系統服務可替透過撥號或寬頻連線所連接的家庭或小型辦公室網路內的所有電腦，提供網路位址轉譯 (NAT)、定址和名稱解析、侵入防止服務。基礎伺服器環境並不需要這些功能。因此，此服務將設成停用(Disabled)。

網站間訊息傳輸

表 3.157：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
IsmServ	停用 (針對網域控制站啟動)	停用	停用	停用

Intersite Messaging (網站間訊息傳輸) 系統服務可讓執行 Windows 伺服器網站的電腦間能互相交換訊息。此服務可用於網站間的郵件型態複寫。Active Directory 可透過在 IP transport 上使用 SMTP，支援網站間的複寫。基礎伺服器環境並不需要這些功能。因此，此服務將設成停用(Disabled)。不過，網域控制站上需要此服務。基於此理由，本手冊所定義三個系統環境中的網域控制站都將 Intersite Messaging 服務設成自動(Automatic)。

IP Version 6 Helper Service

表 3.158：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
6to4	未安裝	停用	停用	停用

IP Version 6 Helper Service 系統服務在現有的 IPv4 網路上提供 IPv6 連線。基礎伺服器環境並不需要這些功能。因此，此服務將設成停用(Disabled)。

IPSEC 原則代理程式 (IPSec Service)

表 3.159：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
PolicyAgent	自動	自動	自動	自動

IPSEC Policy Agent (IPSEC 原則代理程式) 服務可在 TCP/IP 網路上的用戶端和伺服器之間提供端對端的安全性。它也可管理 IP 安全性 (IPSec) 原則，啟動 Internet Key Exchange (IKE)，並與 IP 安全性驅動程式協調 IPSec 原則設定。在本手冊所定義的三個系統環境中都將此服務啟用(Enabled)。

原則代理程式

表 3.160：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Kdc	停用	停用	停用	停用

Kerberos Key Distribution Center (Kerberos 金鑰發行中心) 系統服務可讓使用者以 Kerberos v5 驗證通訊協定登入至網路。基於這些理由，請在網域控制站的原則內，將此服務的值設成自動 (Automatic)。

授權登入服務

表 3.161：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
LicenseService	停用	停用	停用	停用

License Logging Service (授權登入服務) 可替作業系統的某些部分監視和記錄用戶端存取授權。這些包括了 IIS、Terminal Server、檔案/列印，以及不屬於作業系統的產品，例如 SQL Server 和 Microsoft Exchange Server。本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

邏輯磁碟管理員

表 3.162：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Dmserver	自動	手動	手動	手動

Logical Disk Manager (邏輯磁碟管理員) 系統服務可偵測與監視新的硬碟機，並傳送磁碟區資訊給 Logical Disk Manager Administrative Service 來設定組態。此服務會監看所偵測新磁碟機的隨插即用 (Plug and Play) 事件，並將磁碟區和磁碟資訊傳給 Logical Disk Manager Administrative Service 來進行設定。因此，本手冊所定義的三個系統環境都將此服務設成手動(Manual)。

Logical Disk Manager Administrative Service

表 3.163：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Dmadmin	手動	手動	手動	手動

Logical Disk Manager Administrative Service (邏輯磁碟管理員管理服務) 可執行磁碟管理要求的管理服務，並設定硬碟機和磁碟區。Logical Disk Manager Administrative Service 只能啟動於您設定磁碟機或分割，或是偵測到新的磁碟機時。因此，本手冊所定義的三個系統環境都將此選項設成手動(Manual)。

Message Queuing

表 3.164：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Msmq	未安裝	停用	停用	停用

Message Queuing 系統服務是一個訊息處理基礎結構與開發工具，可替 Windows 建立分散式訊息應用程式。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

訊息佇列下層用戶端

表 3.165：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
mqds	未安裝	停用	停用	停用

Message Queuing Down Level Clients (訊息佇列下層用戶端) 系統服務可替網域控制站上的 Message Queuing 用戶端 (Windows 9x、Windows NT 4.0 和 Windows 2000) 提供 Active Directory 存取。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此選項設成停用(Disabled)。

訊息佇列觸發程序

表 3.166：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Mqtsvc	未安裝	停用	停用	停用

Message Queuing Triggers (訊息佇列觸發程序) 系統服務提供以規則方式監視到達 Message Queuing 佇列的訊息，並且只要規則的條件一滿足，就啓用 COM 元件或獨立的可執行程式來處理訊息。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

Messenger

表 3.167：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Messenger	停用	停用	停用	停用

Messenger 系統服務會在用戶端和伺服器之間傳輸與傳送 Alerter 服務訊息。此服務與 Windows Messenger 無關。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

Microsoft POP3 服務

表 3.168：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
POP3SVC	未安裝	停用	停用	停用

Microsoft POP3 Service (Microsoft POP3 服務) 提供電子郵件傳輸和擷取服務。管理員可使用 POP3 服務來儲存和管理郵件伺服器上的電子郵件帳戶。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用 (Disabled)。

MSSQL\$UDDI

表 3.170：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
MSSQL\$UDDI	未安裝	停用	停用	停用

MSSQL\$UDDI 系統服務 — Universal Description Discovery and Integration (UDDI) – 是發行和尋找有關 Web 服務資訊的業界規格。Windows Server 2003 家族包括了 UDDI Services，這是提供 UDDI 能力的 Web 服務，以便用於企業內或組織之間。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

MSSQL Server AD Helper

表 3.171：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
MSSQLServerADHelper	未安裝	停用	停用	停用

MSSQLServerADHelper 系統服務啟用 SQL Server 與 SQL Server Analysis Services，以便當服務並非執行於 LocalSystem 帳戶底下時，在 Active Directory 中發行資訊。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

.NET Framework 支援服務

表 3.172：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
CORRTSvc	未安裝	停用	停用	停用

.NET Framework Support Service (.NET Framework 支援服務) 系統服務會在指定的處理序初始化 Client Runtime Service 時，通知訂閱的用戶端。.NET Framework Support Service 提供了一個稱為 Common Language Runtime 的 Run-Time 環境，它可管理程式碼的執行，並提供可讓開發流程更容易的服務。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

Netlogon

表 3.173：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Netlogon	自動	自動	自動	自動

Netlogon 系統服務可在您的電腦和網域控制站之間維護一個安全的通道，以便驗證使用者和服務。若停用此服務，系統網路上的電腦並不能驗證使用者和服務，而網域控制站也不能註冊 DNS 記錄。特別要注意的是，停用此服務可能會拒絕 NTLM 驗證要求，而在網域控制站的狀況中，它們將無法被用戶端電腦發現。基於這些理由，請將此服務的值設成自動 (Automatic)。

Net Meeting 遠端桌面共

表 3.174：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
mnmsrvc	停用	停用	停用	停用

NetMeeting Remote Desktop Sharing (NetMeeting 遠端桌面共用) 系統服務可透過在公司 intranet 上使用 Microsoft NetMeeting[®]，讓授權的使用者從遠端存取此電腦。此服務必須明確地由 NetMeeting 所啟用，並可在 NetMeeting 中停用，或透過 Windows 工作列圖示來關機。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

網路連線

表 3.175：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Netman	手動	手動	手動	手動

Network Connections (網路連線) 服務可管理 Network Connections 資料夾內的物件，您可在其中檢視網路和遠端連線這兩者。當啟動類型為手動(Manual)，並且 Network Connections 介面啓用時，此服務將會自動啓動。本手冊所定義的三個系統環境都將此服務設成手動(Manual)。

網路 DDE

表 3.176：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
NetDDE	停用	停用	停用	停用

Network DDE (網路 DDE) 系統服務可替執行於同一台電腦或不同電腦上的程式提供 Dynamic Data Exchange (動態資料交換，簡寫為 DDE) 的網路傳輸和安全性。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

Network DDE DSDM

表 3.177：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
NetDDEdsdm	停用	停用	停用	停用

Network DDE DSDM (網路 DDE DSDM) 系統服務可管理 DDE 網路共用區。此服務只能供 Network DDE 服務用來管理共用的 DDE 交談。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用 (Disabled)。

Network Location Awareness (NLA)

表 3.178：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
NLA	手動	手動	手動	手動

Network Location Awareness (網路位置感知，簡寫為 NLA) 系統服務會收集和儲存網路組態資訊，例如 IP 位址和網域名稱變更，以及位置變更資訊，並在此資訊變更時通知應用程式。停用此服務將令您無法找到網路，並且任何明確倚賴它的服務都將無法啟動。基礎伺服器環境可能需要這些功能。基於這些理由，本手冊所定義的三個系統環境都將此服務設成手動(Manual)。

網路新聞傳輸通訊協定 (NNTP)

表 3.179：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
NntpSvc	未安裝	停用	停用	停用

Network News Transport Protocol (網路新聞傳輸通訊協定，簡寫為 NNTP) 系統服務可讓執行 Windows Server 2003 的電腦作為新聞伺服器。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

NTLM 安全性支援提供者

表 3.180：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
NtLmSsp	未安裝	自動	自動	自動

NTLM Security Support Provider (NTLM 安全性支援提供者) 系統服務提供安全性給使用傳輸、而非具名管道 (Named Pipe) 的 RPC 程式，並讓使用者使用 NTLM 驗證通訊協定來登入至網路。NTLM 通訊協定會驗證不使用 Kerberos v5 版驗證的用戶端。若停用此服務，使用者將無法使用 NTLM 驗證通訊協定登入至用戶端，或存取網路資源。因此，本手冊所定義的三個系統環境都將此選項設成自動(Automatic)。

效能記錄檔和警示

表 3.181：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
SysmonLog	手動	手動	手動	手動

Performance Logs and Alerts (效能記錄檔和警示) 系統服務會根據預先設定的排程參數，向本機或遠端電腦收集效能資料，接著將資料寫至記錄檔或觸發一個警示。基礎伺服器環境需要這些功能。因此，本手冊所定義的三個系統環境都將此服務設成手動 (Manual)。

隨插即用

表 3.182：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
PlugPlay	自動	自動	自動	自動

Plug and Play (隨插即用) 系統服務可讓電腦辨識硬體變更，並隨之做調整，使用者完全不需輸入任何資料，或只需輸入少數資料。若此服務是透過 MSCONFIG 疑難排解工具來停止，裝置管理員介面將顯示成空白，並且不會顯示任何硬體裝置。因此，本手冊所定義的三個系統環境都將此服務設成自動 (Automatic)。

可攜式媒體序號

表 3.183：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
WmdmPmSN	手動	停用	停用	停用

Portable Media Serial Number (可攜式媒體序號) 系統服務可擷取連至您電腦的任何可攜式音樂播放程式的序號。基礎伺服器環境並不需要這些功能。因此，本手冊所定義的三個系統環境都將此服務設成停用 (Disabled)。

Macintosh 的列印伺服器

表 3.184：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
MacPrint	未安裝	停用	停用	停用

Print Server for Macintosh (Macintosh 的列印伺服器) 系統服務可讓 Macintosh 用戶端將列印工作路由至執行 Windows Server 2003 Enterprise Server 的電腦上的列印多工緩衝處理器。基礎伺服器環境並不需要這些功能。因此，本手冊所定義的三個系統環境都將此服務設成停用 (Disabled)。

列印多工緩衝處理器

表 3.185：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Spooler	自動	停用	停用	停用

Print Spooler (列印多工緩衝處理器) 系統服務管理所有本機與網路的列印佇列，並控制所有的列印工作。基礎伺服器環境並不需要這些功能。因此，此服務將設成停用 (Disabled)。不過，列印伺服器角色會將此服務設成自動 (Automatic)。如需要更多關於此伺服器角色的資訊，請參閱第七章「補強列印伺服器」。

受保護的儲存區

表 3.186：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
ProtectedStorage	自動	自動	自動	自動

Protected Storage (受保護的儲存區) 系統服務可保護私密金鑰等敏感資訊的儲存區，並防止被未授權的服務、處理序或使用者存取。若停用此服務，私密金鑰將無法存取、認證伺服器無法運作、S/MIME 和 SSL 無法作用、智慧卡登入也會失敗。基於這些理由，請將此服務的值設成自動(Automatic)。

遠端存取自動連線管理員

表 3.187：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
RasAuto	手動	停用	停用	停用

Remote Access Auto Connection Manager (遠端存取自動連線管理員) 系統服務可偵測連至遠端網路或電腦的失敗嘗試，接著提供替代作法來進行連線。Remote Access Auto Connection Manager 服務可在每次程式無法參照到遠端 DNS 或 NetBIOS 名稱或位址時，以撥號或虛擬私人網路 (VPN) 連線連到遠端網路。基礎伺服器環境並不需要這些功能。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

遠端存取連線管理員

表 3.188：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
RasMan	手動	停用	停用	停用

Remote Access Connection Manager (遠端存取連線管理員) 系統服務可管理從您的電腦連至 Internet 或其他遠端網路的撥號和 VPN 連線。基礎伺服器環境並不需要這些功能。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

遠端管理服務

表 3.189：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
SrvcSurg	未安裝	手動	手動	手動

Remote Administration Service (遠端管理服務) 系統服務將在伺服器重新啟動時，執行下列的遠端管理工作：

- 增加伺服器的開機計數。
- 若日期和時間未設定於伺服器上，將會引發一個警示。
- 若事件電子郵件通知功能尚未設定，將會引發一個警示。

本手冊所定義的三個系統環境都將此服務設成手動 (Manual)。

Remote Desktop Help Session Manager

表 3.190：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
RDSessMgr	手動	停用	停用	停用

Remote Desktop Help Session Manager 系統服務可管理及控制「說明及支援中心」應用程式 (helpctr.exe) 中的遠端協助功能。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

遠端安裝服務

表 3.191：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
BINSVC	未安裝	停用	停用	停用

Remote Installation Services (遠端安裝服務，簡寫為 RIS) 系統服務是包含於 Windows Server 系統之成員內的 Windows 部署功能。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

遠端程序呼叫定位器

表 3.192：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
RpcSs	自動	自動	自動	自動

Remote Procedure Call (遠端程序呼叫，簡寫為 RPC) 系統服務是一個安全的處理序間通訊 (Inter-Process Communication，簡寫為 IPC) 機制，可啟用不同處理序內的資料交換和功能引動。不同的處理序可發生於相同的電腦、區域網路 (LAN) 或 Internet 上。此服務不應該停用。停用 Remote Procedure Call (RPC) 服務將導致作業系統無法載入多個倚賴它的服務。因此，本手冊所定義的三個系統環境都將此服務設成自動(Automatic)。

遠端程序呼叫 (RPC) 定位器

表 3.193：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
RpcLocator	手動(若是在網域控制站 上則為自動)	停用	停用	停用

Remote Procedure Call (RPC) Locator (遠端程序呼叫 (RPC) 定位器) 系統服務可讓 RPC 用戶端能使用 RpcNs* 家族的 API 找到 RPC 伺服器並管理 RPC 名稱服務資料庫。基礎伺服器環境並不需要這些功能。因此，此服務將設成停用(Disabled)。不過，由於網域控制站需要此系統服務，因此將它設成自動(Automatic)。

遠端登錄服務

表 3.194：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
RemoteRegistry	自動	自動	自動	自動

假設遠端使用者擁有必要的權限，Remote Registry Service (遠端登錄服務) 系統服務可讓遠端使用者修改電腦上的登錄設定值。此服務主要是由遠端管理員和效能計數器所使用。若 Remote Registry Service 停用，只有本機電腦容許修改登錄，而任何明確倚賴此服務的服務都將無法啟動。因此，本手冊所定義的三個系統環境都將此服務設成自動(Automatic)。

遠端伺服器管理員

表 3.195：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
AppMgr	未安裝	停用	停用	停用

Remote Server Manager (遠端伺服器管理員) 可作為 Remote Administration Alert Objects (遠端管理警示物件) 的 Windows Management Instrumentation (WMI) 執行個體提供者，和 Remote Administration Tasks 的 WMI 方法提供者。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

遠端伺服器監視器

表 3.196：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Appmon	未安裝	停用	停用	停用

Remote Server Monitor (遠端伺服器監視器) 系統服務可在遠端管理的伺服器上監視重要的系統資源，並管理選擇性的監視程式 (Watchdog) 計時器硬體。基礎伺服器環境並不需要這些功能。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

遠端儲存通知

表 3.197：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Remote_Storage_User_Link	未安裝	停用	停用	停用

Remote Storage Notification (遠端儲存通知) 系統服務會在您讀取或寫入只有輔助儲存媒體才有提供的檔案時通知您。基礎伺服器環境並不需要這些功能。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

遠端儲存伺服器

表 3.198：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Remote_Storage_Server	未安裝	停用	停用	停用

Remote Storage Server (遠端儲存伺服器) 系統服務會將不常用的檔案存到輔助儲存媒體內。此服務可讓 Remote Storage Notification (遠端儲存通知) 在離線檔案被存取時通知使用者。基礎伺服器環境並不需要這些功能。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

抽取式儲存區

表 3.199：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
NtmsSvc	手動	停用	停用	停用

Removable Storage (抽取式儲存區) 系統服務可管理抽取式媒體與替它製作目錄，並操作自動化的抽取式媒體裝置。此服務維護了一個目錄來識別您電腦所使用抽取式媒體 (包括磁帶和 CD) 的資訊。基礎伺服器環境並不需要這些功能。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

重要：使用 Ntbackup.exe 來進行系統備份時需要此服務 – 若您正使用 Ntbackup.exe，請將此服務設成手動(Manual)。

原則提供者的結果集

表 3.200：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
RsoPProv	手動	停用	停用	停用

Resultant Set of Policy Provider (原則提供者的結果集) 系統服務可讓您連至 Windows Server 2003 網域控制站、存取該電腦的 WMI 資料庫、並模擬群組原則設定的 Resultant Set of Policy (RSOP)，以套用至位於 Windows 2000 或以後版本之網域上的 Active Directory 內的使用者或電腦。這通常稱為規劃模式。基礎伺服器環境並不需要這些功能。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

路由與遠端存取

表 3.201：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
RemoteAccess	停用	停用	停用	停用

Routing and Remote Access (路由與遠端存取) 系統服務提供多重通訊協定 LAN-to-LAN、LAN-to-WAN、VPN 和 NAT 路由服務。此外，此服務也提供撥號和 VPN 遠端存取服務。基礎伺服器環境並不需要這些功能。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

SAP 代理程式

表 3.202：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Nwsapagent	未安裝	停用	停用	停用

SAP Agent (SAP 代理程式) 系統服務可使用 IPX Service Advertising Protocol (IPX SAP) 通訊協定在 IPX 網路上廣告網路服務。基礎伺服器環境並不需要這些功能。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

第二次登入

表 3.203：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Seclogon	自動	停用	停用	停用

Secondary Logon (第二次登入) 系統服務可讓使用者在不同安全性主角的環境之中建立處理序。受限制的使用者通常會使用此服務登入成具有較高權限的使用者，以便暫時執行管理程式。此服務可讓使用者在替代的憑證底下啟動處理序。基礎伺服器環境並不需要這些功能。雖然此服務對於用戶端電腦很有用，但它並不適用於大多數的伺服器，因為以互動方式登入至這些伺服器的使用者將成為 IT 團隊的成員，IT 團隊常會執行一些通常需要管理權限的維護工作。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

安全性帳戶管理員

表 3.204：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
SamSs	自動	自動	自動	自動

Security Accounts Manager (安全性帳戶管理員，簡寫為 SAM) 系統服務是一個管理使用者和群組帳戶資訊的受保護子系統。在 Windows 2000 和 Windows Server 2003 系統中，本機電腦登錄中的 SAM 儲存了工作站安全性帳戶，而網域控制站帳戶則儲存於 Active Directory 之中。此服務不可停用。

伺服器

表 3.205：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Lanmanserver	自動	自動	自動	自動

Server (伺服器) 系統服務在網路上提供了 RPC 支援、檔案、列印和具名管道共用。基於這些理由，建議您在本手冊所定義的三個系統環境中將此服務的值設成自動(Automatic)。

核心硬體偵測

表 3.206：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
ShellHWDetection	自動	停用	停用	停用

Shell Hardware Detection (核心硬體偵測) 系統服務會監視與提供有關 AutoPlay 硬體事件的通知。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

簡單郵件傳輸通訊協定

表 3.207：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
SMTPSVC	未安裝	停用	停用	停用

Simple Mail Transport Protocol (簡單郵件傳輸通訊協定，簡寫為 SMTP) 系統服務會在網路上傳送電子郵件。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

簡單 TCP/IP 服務

表 3.208：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
SimpTcp	未安裝	停用	停用	停用

Simple TCP/IP Services (簡單 TCP/IP 服務) 系統服務可支援下列的 TCP/IP 通訊協定：

- Echo (port 7, RFC 862)。
- Discard (port 9, RFC 863)。
- Character Generator (port 19, RFC 864)。
- Daytime (port 13, RFC 867)。
- Quote of the Day (port 17, RFC 865)。

基礎伺服器環境並不需要這些功能。因此，本手冊所定義的三個系統環境都將此服務設成停用 (Disabled)。

單一執行個體儲存區

表 3.209：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Groveler	未安裝	停用	停用	停用

Single Instance Storage Groveler (SIS) (單一執行個體儲存區 Groveler (SIS)) 系統服務是 Remote Installation Service (遠端安裝服務，簡寫為 RIS) 的整合元件，可減少 RIS 磁碟區所需的整體儲存區。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

智慧卡

表 3.210：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
ScardSvr	手動	停用	停用	停用

Smart Card (智慧卡) 系統服務可管理與控制如何存取插入您電腦之智慧卡讀取器內的智慧卡。若停用此服務，您系統環境中的電腦將無法讀取智慧卡。此外，任何明確倚賴它的服務都將無法啟動。基礎伺服器環境並不需要這些功能。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

注意：若主要角色想要進行驗證，其驗證形式之一為透過展示兩個識別因數來確認其身份。通常這牽涉到顯示您知道的某些資料並搭配您擁有的某個物件，例如，將智慧卡插入電腦內，並輸入該卡的 PIN。通常用來證明某人身份的第三個因數是展示您是什麼；這類型的雙因數驗證範例之一是，要求使用者接受視網膜掃描器 (Retina Scanner) 的檢查，之後再輸入其密碼，如此他們方能存取受限制的資源。使用智慧卡來實作多重因數驗證將是最佳作法，並將部署至所有的管理員帳戶內。若您的組織運用智慧卡驗證，此服務需要設成手動(Manual)。

SNMP 服務

表 3.211：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
SNMP	未安裝	停用	停用	停用

SNMP Service (SNMP 服務) 可讓傳入的 SNMP 要求由本機電腦所服務。SNMP Service 包含了監視網路裝置內活動的代理程式，並會向網路主控台工作站報告。本手冊所定義的三個系統環境都不需要、也不倚賴 SNMP Server。因此，這三個系統環境都將此服務設成SNMP 服務。

SNMP 陷阱服務

表 3.212：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
SNMPTRAP	未安裝	停用	停用	停用

SNMP Trap Service (SNMP 陷阱服務) 會接收本機或遠端 SNMP 代理程式產生的陷阱訊息，並將訊息轉送給執行於您電腦上的 SNMP 管理程式。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

特殊管理主控台 Helper

表 3.213：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Sacsvr	手動	停用	停用	停用

若任一個作業系統的 Windows Server 2003 系統由於 Stop (停止) 錯誤訊息而停止運作，Special Administration Console Helper (特殊管理主控台 Helper) 系統服務 (SAC) 可執行遠端管理工作。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

SQLAgent\$* (*UDDI or WebDB)

表 3.214：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
SQLAgent\$WEB DB	未安裝	停用	停用	停用

SQLAgent\$* (* UDDI or WebDB) (SQLAgent\$* (* UDDI 或 WebDB)) 是一個工作排程器與監視服務。它也可在執行 SQL Server 的電腦之間移動資訊，並大量地用於備份和複寫。若停止 SQLAgent\$* (* UDDI or WebDB) 服務，SQL 複寫將不會發生。此外，這也會損害到所有排程的工作和警示/事件監視，以及自動重新啟動 SQL Server 服務。若此服務停用，任何明確倚賴此服務的服務都將無法啟動。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

系統事件通知

表 3.215：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
自動	自動	自動	自動	自動

System Event Notification (系統事件通知) 系統服務可監視和追蹤系統事件，例如 Windows 登入網路和電源事件，接著將這些事件通知 COM+ 事件系統訂閱者。本手冊所定義的三個系統環境都將此服務設成自動(Automatic)。

工作排程器

表 3.216：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Schedule	自動	停用	停用	停用

Task Scheduler (工作排程器) 系統服務可讓您在電腦上設定與排程自動化的工作。Task Scheduler 服務可監視您選擇的任何準則，並在準則符合您指定的條件時執行工作。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

重要：若您正使用 Ntbackup.exe 來進行排程的備份，此服務必須設成自動(Automatic)。

TCP/IP NetBIOS Helper 服務

表 3.217：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
LMHosts	自動	自動	自動	自動

TCP/IP NetBIOS Helper Service (TCP/IP NetBIOS Helper 服務) 可在 TCP/IP (NetBT) 服務上支援 NetBIOS，並替您網路上的用戶端提供 NetBIOS 名稱解析；因此可讓使用者共用檔案、列印與登入至網路。本手冊所定義的三個系統環境都將此服務設成自動(Automatic)。

TCP/IP 列印伺服器

表 3.218：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
LPDSVC	未安裝	停用	停用	停用

TCP/IP Print Server (TCP/IP 列印伺服器) 系統服務可讓您使用 Line Printer Daemon 通訊協定來進行 TCP/IP 型態的列印。基礎伺服器環境並不需要此功能。因此，這三個系統環境都將此服務設成停用(Disabled)。

Telephony

表 3.219：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
TapiSrv	手動	停用	停用	停用

Telephony 服務替控制電話裝置的程式提供 API (TAPI) 支援，也可替本機電腦上以及會通過執行該服務之伺服器上 LAN 的 IP 型語音連線提供 API 支援。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

Telnet

表 3.220：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
TlntSvr	停用	停用	停用	停用

Windows 的 Telnet 系統服務可提供 ASCII 終端機工作階段給 Telnet 用戶端。此服務可支援兩類驗證和四類終端機：ANSI、VT-100、VT-52 和 VTNT。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

終端機服務

表 3.221：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
TermService	手動	自動	自動	自動

Terminal Services (終端機服務) 系統服務提供了多重工作階段的環境，可讓用戶端裝置存取執行於伺服器上的虛擬 Windows 桌面工作階段和 Windows 型態的程式。Terminal Services 可讓多重使用者以互動方式連至一台電腦，並在遠端電腦上顯示桌面和應用程式。在預設狀態下，Terminal Services 系統服務將安裝在遠端管理模式。若要在應用程式模式中安裝 Terminal Services，請使用 Configure Your Server 或 Add/Remove Windows Components 來變更 Terminal Services 模式。因為此服務是從遠端管理伺服器的強大工具，本手冊所定義的三個系統環境都將它設成自動(Automatic)。

注意：要防止在您的環境中遠端使用電腦，請在 System properties 對話方塊的 Remote 索引標籤中清除「Allow Remote Assistance」與「Allow Remote Desktop」核取方塊。

終端機服務授權

表 3.222：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
TermServLicensing	未安裝	停用	停用	停用

Terminal Services Licensing (終端機服務授權) 系統服務會在連至終端機伺服器時安裝一個授權的伺服器，並提供註冊過的用戶端授權。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

終端機服務工作階段目錄

表 3.223：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Tssdis	停用	停用	停用	停用

Terminal Services Session Directory (終端機服務工作階段目錄) 系統服務提供了多重工作階段環境，可讓用戶端裝置存取虛擬的 Windows 桌面工作階段和 Windows Server 2003 上的 Windows 型態程式。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

Themes

表 3.224：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Themes	停用	停用	停用	停用

Themes (主題) 系統服務提供使用者經驗主題管理服務。Themes 服務可替新的 Windows XP Professional 圖形使用者介面 (GUI) 提供呈現支援。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

瑣碎 FTP Daemon

表 3.225：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
tftpd	未安裝	停用	停用	停用

Trivial FTP Daemon (瑣碎 FTP Daemon，簡稱為 TFTP) 系統服務並不需要使用者名稱或密碼，並且為 RIS 不可或缺的一部分。Trivial FTP Daemon 服務實作了下列 RFC 所定義 TFTP 通訊協定的支援：

- RFC 1350 - TFTP。
- RFC 2347 – 選項擴充功能。
- RFC 2348 – 區塊大小選項。
- RFC 2349 – 逾時間隔和傳輸大小選項。

若停用此服務，向此伺服器要求 RIS 的用戶端電腦將無法安裝。不過，基礎伺服器環境並不需要此功能。因此，這三個系統環境都將此服務設成停用(Disabled)。

不斷電供電

表 3.226：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
UPS	手動	停用	停用	停用

Uninterruptible Power Supply (不斷電供電) 系統服務可管理透過序列埠連至您電腦的不斷電供電系統 (UPS)。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

上載管理員

表 3.227：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Uploadmgr	手動	停用	停用	停用

Upload Manager (上載管理員) 系統服務可管理網路上用戶端和伺服器之間的同步和非同步檔案傳輸。驅動程式資料可以非同步地從客戶電腦上載至 Microsoft，接著用來協助使用者尋找其系統所需的驅動程式。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

虛擬磁碟服務

表 3.228：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
VDS	手動	停用	停用	停用

Virtual Disk Service (虛擬磁碟服務，簡寫為 VDS) 系統服務可提供單一介面來管理區塊儲存區虛擬化，不管它是進行於作業系統軟體內、獨立磁碟多餘陣列 (RAID) 儲存硬體子系統、或其他的虛擬引擎。基礎伺服器環境並不需要這些功能。因此，這三個系統環境都將此服務設成停用(Disabled)。

磁碟區陰影複製

表 3.229：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
VSS	手動	手動	手動	手動

Volume Shadow Copy (磁碟區陰影複製) 系統服務可管理與實作磁碟區陰影複本，以用於備份和其他用途。此服務是基礎伺服器原則的核心必要項目。因此，本手冊所定義的三個系統環境都將此服務設成手動(Manual)。

Web Client

表 3.230：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
WebClient	停用	停用	停用	停用

WebClient 系統服務可讓 Win32 應用程式存取 Internet 上的文件。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

Web 元件管理員

表 3.231：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Elementmgr	未安裝	停用	停用	停用

Web Element Manager (Web 元件管理員) 系統服務負責替連接埠 8098 的管理網站提供 Web 使用者介面項目。基礎伺服器環境並不需要此功能。因此，這三個系統環境都將此服務設成停用(Disabled)。

Windows 音訊

表 3.232：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
AudioSrv	停用	停用	停用	停用

Windows Audio (Windows 音訊) 系統服務可支援聲音和相關的 Windows 音訊事件功能。基礎伺服器環境並不需要此功能。因此，這三個系統環境都將此服務設成停用(Disabled)。

影像擷取 (WIA)

表 3.233：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
StiSvc	停用	停用	停用	停用

Windows Image Acquisition (Windows 影像擷取，簡寫為 WIA) 系統服務可替掃描器和相機提供影像擷取服務。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

Windows 安裝程式

表 3.234：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
MSIServer	手動	自動	自動	自動

Windows Installer (Windows 安裝程式) 系統服務將在安裝過程中套用一組集中定義的設定規則，藉此管理應用程式的安裝與移除。基礎伺服器環境需要此服務；因此，本手冊所定義的三個系統環境都將它設成自動(Automatic)。

Windows 網際網路名稱服務 (WINS)

表 3.235：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
WINS	未安裝	停用	停用	停用

Windows Internet Name Service (Windows 網際網路名稱服務，簡寫為 WINS) 系統服務可啟用 NetBIOS 名稱解析。WINS 伺服器是否存在，對於尋找以 NetBIOS 名稱來辨識的網路資源相當重要。除非所有網域都已升級至 Active Directory，並且網路上所有的電腦都執行 Windows Server 2003，否則就一定需要 WINS。基礎伺服器環境並不需要這些功能。因此，建議您將此服務的值設成停用(Disabled)。Infrastructure Server (基礎架構伺服器) 角色原則也將此服務設成自動(Automatic)。

Windows 管理追蹤記錄

表 3.236：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
winmgmt	自動	自動	自動	自動

Windows Management Instrumentation (Windows 管理追蹤記錄) 系統服務提供常見的介面和物件模型來存取有關作業系統、裝置、應用程式和服務的管理資訊。WMI 是一個建立管理應用程式和追蹤記錄的基礎架構，是由新一代的 Microsoft 作業系統所提供。若停用此服務，大多數的 Windows 軟體將無法正常運作，並且任何明確倚賴它的服務都將無法啟動。因此，本手冊所定義的三個系統環境都將此服務設成自動(Automatic)。

Windows 管理追蹤記錄驅動程式擴充功能

表 3.237：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Wmi	手動	手動	手動	手動

Windows Management Instrumentation Driver Extensions (Windows 管理追蹤記錄驅動程式擴充功能) 系統服務會監視已設成要發行 WMI 或事件追蹤資訊的所有驅動程式和事件追蹤提供者。本手冊所定義的三個系統環境都將此服務設成手動(Manual)。

Windows 媒體服務

表 3.238：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
WMServer	未安裝	停用	停用	停用

Windows Media Services (Windows 媒體服務) 系統服務可在 IP 型態的網路上提供資料流媒體服務。此服務可取代組成 Windows Media Services 4.0 和 4.1 版的四個個別服務：Windows Media Monitor Service、Windows Media Program Service、Windows Media Station Service 和 Windows Media Unicast Service。基礎伺服器環境並不需要此功能。因此，這三個系統環境都將此服務設成停用(Disabled)。

Windows 系統資源管理員

表 3.239：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
WindowsSystemResourceManager	未安裝	停用	停用	停用

Windows System Resource Manager (Windows 系統資源管理員，簡寫為 WSRM) 系統服務是一個可協助客戶將應用程式部署到整合案例中的工具。基礎伺服器環境並不需要此功能。因此，這三個系統環境都將此服務設成停用(Disabled)。

Windows 時間

表 3.240：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
W32Time	自動	自動	自動	自動

Windows Time (Windows 時間) 系統服務可在所有執行於 Windows 網路上的電腦間維持日期和時間的同步化。它使用 Network Time Protocol (網路時間通訊協定，簡寫為 NTP) 來將電腦時鐘同步化，以便針對網路驗證和資源存取要求提供準確的時鐘值，亦即時間戳記。它是在 Active Directory 網域內提供可靠 Kerberos 驗證的核心需求，因此，本手冊所定義的三個系統環境都將此服務設成自動(Automatic)。

WinHTTP Web Proxy 自動探索服務

表 3.241：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
WinHttpAutoProxySvc	手動	停用	停用	停用

WinHTTP Web Proxy Auto-Discovery Service (WinHTTP Web Proxy 自動探索服務) 系統服務可替 Windows HTTP 服務 (WinHTTP) 實作 Web Proxy Auto-Discovery (WPAD) 通訊協定。WPAD 是一個可讓 HTTP 用戶端自動探索 proxy 組態的通訊協定。基礎伺服器環境並不需要此功能。因此，這三個系統環境都將此服務設成停用(Disabled)。

無線零組態

表 3.242：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
WZCSVC	在 Standard、Enterprise 和 Datacenter Server 上為自動。在 Web Server 上為手動	停用	停用	停用

Wireless Zero Configuration (無線零組態) 系統服務可啓用 IEEE 802.11 無線介面卡的自動組態，以進行無線的通訊。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

WMI 效能配接器

表 3.243：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
WmiApSrv	Manual 手動	停用	停用	停用

WMI Performance Adapter (WMI 效能配接器) 系統服務提供了來自 WMI HiPerf 提供者的效能程式庫資訊。此服務是一個手動服務，在預設狀態下並不會執行。它可依需要執行於效能用戶端 (例如 Sysmon) 使用 Performance Data Helper (PDH) 來查詢效能資料時。一旦用戶端中斷連線後，此服務就會停止。若停用此服務，WMI 效能計數器將無法使用。因此，本手冊所定義的三個系統環境都將此服務設成手動 (Manual)。

工作站

表 3.244：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
Lanmanworkstation	自動	自動	自動	自動

Workstation (工作站) 系統資源會建立與維護用戶端網路連線和通訊。若停用此服務，您就無法與遠端伺服器建立連線，也無法透過具名管道來存取檔案。因此，本手冊所定義的三個系統環境都將此服務設成自動(Automatic)。

全球資訊網發行服務

表 3.245：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
W3SVC	未安裝	停用	停用	停用

World Wide Web Publishing Service (全球資訊網發行服務) 系統服務透過 Internet Information Service 嵌入式管理單元提供了 Web 連線和管理。此服務並非基礎伺服器原則的必要項目。因此，本手冊所定義的三個系統環境都將此服務設成停用(Disabled)。

其他登錄設定

系統會針對基礎安全性範本檔來建立額外的登錄值項目，本手冊所定義的三個安全性環境的管理範本 (Administrative Template) (.adm) 檔案中並沒有定義它們。這些 .adm 檔定義了有關 Windows Server 2003 的桌面、shell 及安全性設定的系統原則和限制。

這些設定都內嵌於安全性範本的 Security Options (安全性選項) 區內，以便將變更自動化。若移除了此原則，它的設定並不會自動被移除，必須用 Regedt32.exe 等類的登錄編輯工具手動變更。相同的登錄值將套用到三個系統環境之中。

本手冊透過修改 %windir%\inf 資料夾內的 sceregl.inf 和重新註冊 scecli.dll，將額外的設定加至 Security Configuration Editor (SCE) 內。原本的安全性設定值以及額外的設定值都將出現在本章先前所列的嵌入式管理單元和工具的 Local Policies\Security 底下。您應更新 sceregl.inf 檔，並在任何將會編輯本手冊所提供安全性範本和群組原則的電腦上重新註冊 scecli.dll，如同所附的手冊所述：《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》，網址為：

<http://go.microsoft.com/fwlink/?LinkId=15159>。

本章節只概述了這些額外的登錄值，所附的手冊中將更完整地說明它們。如需預設設定的相關資訊，及此節所討論的每個設定的詳細說明資訊，請參閱所附手冊《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》，網址為：<http://go.microsoft.com/fwlink/?LinkId=15159>。

網路攻擊的安全性考量

表 3.246：設定值

子機碼登錄值項目	格式	舊版用戶端	企業用戶端	高安全性
EnableICMPRedirect	DWORD	0	0	0
SynAttackProtect	DWORD	1	1	1
EnableDeadGWDetect	DWORD	0	0	0
EnablePMTUDiscovery	DWORD	0	0	0
KeepAliveTime	DWORD	300,000	300,000	300,000
DisableIPSourceRouting	DWORD	2	2	2
DTcpMaxConnectResponse Retransmissions	DWORD	2	2	2
TcpMaxDataRetransmissions	DWORD	3	3	3
PerformRouterDiscovery	DWORD	0	0	0
TCPMaxPortsExhausted	DWORD	5	5	5

Denial of service (拒絕服務，簡寫為 DoS) 攻擊指的是一種讓電腦或電腦上的特定服務無法提供使用者網路服務的網路攻擊。DoS 攻擊可能很難防禦。為協助防止這些攻擊，您應使用最新的安全性修復項目來更新您的電腦，並補強執行 Windows Server 2003 的電腦上的 TCP/IP 通訊協定堆疊，因為這些電腦都暴露於潛在的攻擊之下。預設的 TCP/IP 堆疊組態已調整成可處理標準的 intranet 傳輸。若您將電腦直接連至 Internet，Microsoft 會建議您補強 TCP/IP 堆疊以預防 DoS 攻擊。

下列的登錄值項目已加入 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\登錄機碼內的範本檔之中。

AFD.SYS 設定

表 3.247 設定值

子機碼登錄值項目	格式	舊版用戶端	企業用戶端	高安全性
DynamicBacklogGrowthDelta	DWORD	10	10	10
EnableDynamicBacklog	DWORD	1	1	1
MinimumDynamicBacklog	DWORD	20	20	20
MaximumDynamicBacklog	DWORD	20000	20000	20000

Windows Sockets (Windows 通訊端) 應用程式，例如 FTP 伺服器和 Web 伺服器，都讓 Afd.sys 處理其連線嘗試。Afd.sys 已做過修改，可在半開啓狀態中支援大量連線，並且不會拒絕合法用戶端的存取。其作法是允許管理員設定一個動態的 backlog。Windows Server 2003 包含的 Afd.sys 版本可支援四個登錄參數，以用來控制動態的 backlog 行為。下列的登錄值項目已加入 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\AFD\Parameters\登錄機碼內的範本檔之中：

Configure NetBIOS Name Release Security:

(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers

表 3.248 設定值

子機碼登錄值項目	格式	舊版用戶端	企業用戶端	高安全性
NoNameReleaseOnDemand	DWORD	1	1	1

此項目在 SCE 中將顯示成 “MSS:(NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers”。NetBIOS over TCP/IP 是一個網路通訊協定，它提供了一個方式，可輕鬆地將註冊於 Windows 系統上的 NetBIOS 名稱解析成設定於這些系統上的 IP 位址。此值可決定當電腦收到一個名稱發行要求時，是否要發行其 NetBIOS 名稱。

下列的登錄值項目已加至

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\

登錄機碼內的範本檔之中。

使自動產生的8.3檔案名稱停用:使得電腦停止產生8.3形式的檔案名稱

表 3.249：設定值

子機碼登錄值項目	格式	舊版用戶端	企業用戶端	高安全性
NtfsDisable8dot3NameCreation	DWORD	1	1	1

此項目在 SCE 中將顯示成 “MSS:Enable the computer to stop generating 8.3 style filenames”。Windows Server 2003 支援 8.3 檔案名稱格式，以便提供可與 16-bit 應用程式相容的回溯相容性。8.3 檔案名稱慣例是一個命名格式，它可讓檔案名稱最多包含 8 個字元。下列的登錄值項目已加入 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\FileSystem\ 登錄機碼內的範本檔之中：

停用自動執行:停用所有磁碟機的自動執行程式

表 3.250：設定值

子機碼登錄值項目	格式	舊版用戶端	企業用戶端	高安全性
NoDriveTypeAutoRun	DWORD	0xFF	0xFF	0xFF

此項目在 SCE 中將顯示成 “MSS:Disable Autorun for all drives”。媒體一插入電腦之後，Autorun 就會開始從電腦的磁碟機中讀取資料。因此，程式的安裝檔和音訊媒體上的聲音將會立即啟動。下列的登錄值項目已加至 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\ 登錄機碼內的範本檔之中。

立即執行螢幕保護密碼保護:螢幕保護程式啟動前之寬限秒數 (建議設為0)

表 3.251：設定值

子機碼登錄值項目	格式	舊版用戶端	企業用戶端	高安全性
ScreenSaverGracePeriod	String	0	0	0

此項目在 SCE 中將顯示成 “MSS:The time in seconds before the screen saver grace period expires (0 recommended)”。若啓用螢幕保護程式鎖定，Windows 會在螢幕保護程式啟動和主控台自動鎖定之間加入一段寬限期 (Grace Period)。下列的登錄值項目已加入 HKEY_LOCAL_MACHINE\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\ 登錄機碼內的範本檔之中：

安全性記錄檔接近臨界值之警示:當安全記錄檔達到容量的某一百分比時，產生警示

表 3.252：設定值

子機碼登錄值項目	格式	舊版用戶端	企業用戶端	高安全性
WarningLevel	DWORD	90	90	90

此項目在 SCE 中將顯示成 “MSS:Percentage threshold for the security event log at which the system will generate a warning”。此選項是由 Windows 2000 的 SP3 首先提供，此新功能可在安全性記錄檔到達使用者定義的臨界值之後，在安全性事件記錄檔內產生安全性稽核。例如，若此值設成 90，那麼當安全性記錄檔到達容量的 90 % 之後，將會顯示 eventID 523 事件項目的文字：“The security event log is 90 percent full (安全性事件記錄檔已經到達 90 % 的容量)”。

注意：若您設定了「Overwrite events as needed」或「Overwrite events older than x days」記錄檔設定值，此事件將不會產生。

下列的登錄值項目已加入 HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Services\Eventlog\Security\ 登錄機碼內的安全性範本檔之中。

啓用安全 DLL 搜尋順序:啓動安全 DLL 搜尋模式 (建議)

表 3.253 : 設定值

子機碼登錄值項目	格式	舊版用戶端	企業用戶端	高安全性
SafeDllSearchMode	DWORD	1	1	1

此項目在 SCE 中將顯示成 “MSS:Enable Safe DLL search mode (recommended)”。DLL 搜尋順序可設成採用下列兩種方式，搜尋正在執行之處理序所要求的 DLL：

- 先搜尋系統路徑所指定的資料夾，接著再搜尋目前的工作資料夾。
- 先搜尋目前的工作資料夾，接著再搜尋系統路徑所指定的資料夾。

將登錄值設成 1。當設定值為 1 時，系統會先搜尋系統路徑所指定的資料夾，接著再搜尋目前的工作資料夾。當設定值為 0 時，系統會先搜尋目前的工作資料夾，接著再搜尋系統路徑所指定的資料夾。

下列的登錄值項目已加入 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\登錄機碼內的範本檔之中。

其他安全性設定

雖然在本手冊所定義的三個系統環境中，用來補強基礎伺服器的大多數反制措施都是透過群組原則來套用，但仍有一些額外的設定很難或根本無法以群組原則來套用。如需本章節所探討每個反制措施的詳細說明，請參閱所附的手冊，《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》，網址為：<http://go.microsoft.com/fwlink/?LinkId=15159>。

手動補強程序

本章節將說明如何手動地實作一些額外的反制措施，例如保護帳戶，以及如何使用核心指令碼來讓其他措施正常運作，例如 IPsec 篩選器，以保護本手冊所定義每個安全性環境的 MSBP。

手動地將唯一的安全性群組加至使用者權限

設定

大多數有關使用者權限設定的建議安全性群組都設定於本手冊所附的安全性範本內。不過，有一些權限並無法包含於安全性範本內，因為某些安全性群組的 SID 在不同的 Windows 2003 網域內是唯一的。此問題出在屬於 SID 一部份的唯一 RID (Relative Identifier, 相對識別碼) 是唯一的。這些唯一的執行個體均描述於下表之中。

警告：下表包含了 Built-in Administrator (內建管理員) 的值。Built-in Administrator 是內建的使用者帳戶，而非安全性群組 “Administrators”。若 Administrators 安全性群組已加至底下的任一個拒絕存取使用者權限中，您需要登入至本機，以訂正將 Administrators 群組加至這些權限的錯誤。

此外，Built-in Administrator 帳戶可能會根據以上的建議將您的 Administrator 帳戶重新命名，因此將會擁有新的名稱。在加入此帳戶時，請記得選取重新命名後的管理員帳戶。

表 3.254 手動加入使用者權限設定

UE 中的設定名稱	舊版用戶端	企業用戶端	高安全性
Deny access to this computer from the	內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶	內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶	內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶
Deny log on as a batch job	Support_388945a0 和 Guest	Support_388945a0 和 Guest	Support_388945a0 和 Guest
Deny log on through Terminal Services	內建管理員; Guests; Support_388945a0; Guest; 所有非作業系統服務的 帳戶	內建管理員; Guests; Support_388945a0; Guest; 所有非作業系統服務的 帳戶	內建管理員; Guests; Support_388945a0; Guest; 所有非作業系統服務的 帳戶

重要：所有非作業系統服務的帳戶指的是企業內特定應用程式所使用的服務帳戶。

這並未包含 LOCAL SYSTEM、LOCAL SERVICE 或 NETWORK SERVICE 帳戶，它們都是作業系統使用的內建帳戶。

若要手動地將以上的安全性群組加到企業用戶端 - 成員伺服器基礎原則 (Member Server Baseline Policy) 內，請執行底下的步驟。

- 將安全性群組加至使用者權限設定內

1. 在 Active Directory Users and Computers 中，以滑鼠右鍵按一下 Member Servers OU，然後選取 Properties。
2. 在 Group Policy 索引標籤中選取 Enterprise Client Member Server Baseline Policy 來編輯連結的 GPO。
3. 選取 Enterprise Client - Member Server Baseline Policy，接著按一下編輯(Edit)。
4. 在 Group Policy 視窗中按一下 Computer Configuration\Windows Settings\Security Setting\Local Policies\User Rights Assignment，從上表中替每個權限加入唯一的安全性群組。
5. 關閉修改過的群組原則。
6. 關閉 Member Servers OU Properties 視窗。
7. 在網域控制站之間強迫複製，以透過下列程序讓它們全都套用原則：
 - a. 開啓一個命令提示字元，並使用 gpupdate.exe 命令列工具，強迫網域控制站以下列命令重新整理原則：
gpupdate /Force。
 - b. 將伺服器重新開機，以便讓登錄和服務的變更生效。
8. 在事件記錄檔中確認群組原則已成功地下載，並且該伺服器可以與網域中的其他網域控制站互相通訊。

保護知名帳戶

Windows Server 2003 擁有許多無法刪除、但可重新命名的內建使用者帳戶。Windows 2003 內兩個最有名的內建帳戶為 Guest 與 Administrator。

在預設狀態下，Guest 帳戶在成員伺服器和網域控制站上都是停用的。此設定不應該變更。內建的 Administrator 帳戶應該重新命名，而描述也應改變，以防止駭客使用知名的帳戶危害遠端的伺服器。

許多惡意程式碼的變型都在初次嘗試中使用內建的管理員帳戶來危害伺服器。近年來，此組態變更的價值已逐漸減少，因為現在嘗試侵入伺服器的攻擊工具會指定內建 Administrator 帳戶的 SID 來決定其真正的名稱。SID 指的是可唯一識別網路上每個使用者、群組、電腦帳戶和登入工作階段的數值。您不可能變更此內建帳戶的 SID。將本機管理員帳戶重新命名為唯一的名稱，可讓您的作業群組監視嘗試攻擊此帳戶的事件。

請照以下步驟完成對網域和伺服器上知名帳戶的保護：

1. 在每個網域和伺服器上，重新命名 Administrator 和 Guest 帳戶，並將其密碼變更為長而複雜的值。
2. 在伺服器上使用不同的名稱和密碼。若所有的網域和伺服器上都使用相同的帳戶名稱和密碼，可存取某台成員伺服器的駭客即可以相同的帳戶名稱和密碼來存取所有其他的伺服器。
3. 將帳戶描述變更為預設值以外的值，以防止他人輕易地識別出帳戶。
4. 將這些變更記錄在安全的位置。

注意：內建的 Administrator 帳戶可透過群組原則來重新命名。在 DCBP 中並未實作此項設定，因為您必須為您的環境選擇一個獨特的名稱。Accounts:Rename administrator account 可設成將此手冊所定義三個系統環境中的管理員帳戶重新命名。此設定值是 GPO 的安全性選項設定的一部份。

保護服務帳戶

除非絕對必要，否則千萬不要將服務設定成執行於網域帳戶的安全性內容底下。若伺服器已實體地受到危害，他人即可透過傾印 LSA 秘密，輕鬆取得網域帳戶的密碼。

NTFS

NTFS 分割可在檔案和資料夾層級中支援 ACL。此支援無法用於檔案配置表 (FAT)、FAT32 或檔案系統內。FAT32 是 FAT 檔案系統的一個版本，它已更新成可允許小很多的預設叢集大小，並支援大小高達 2 terabytes 的硬碟。FAT32 包含於 Windows 95 OSR2、Windows 98、Microsoft Windows Me、Windows 2000、Windows XP Professional 和 Windows Server 2003 內。

請使用 NTFS 將每台伺服器上的所有分割格式化。使用 `convert utility` 小心地將 FAT 分割轉換成 NTFS，但是請注意，轉換公用程式會將轉換後磁碟機的 ACL 設成 `Everyone:Full Control`。

對於 Windows 2003 Server 型態的系統而言，請將下列的安全性範本套用至本機，以便個別地替工作站、伺服器和網域

控制站設定預設的檔案系統 ACL：

- %windir%\inf\defltsv.inf
- %windir%\inf\defltdc.inf

注意：預設的網域控制站安全性設定將套用於將伺服器升級到網域控制站時。

本手冊所定義三個系統環境中的伺服器內的所有分割都是以 NTFS 分割來格式化，以透過 ACL 來管理檔案和目錄的安全性。

終端機服務設定

表 3.255 設定值

Setting Name in UE	舊版用戶端	企業用戶端	高安全性
設定用戶端連線加密等級	高	高	高

Set client connection encryption level (設定用戶端連線加密等級) 此設定決定您系統環境中終端機服務用戶端連線的加密等級。High Level (高等級) 設定選項使用 128 位元加密來防止駭客在終端機服務期間使用封包分析程式偷聽。一些較舊版本的終端機服務用戶端並不支援這種高等級的加密。如果您的網路含有這種用戶端，要將傳送和接收資料的加密等級，設在用戶端支援的最高加密等級。

在群組原則中設定此選項的路徑為：

Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security。

共有三個加密等級可用，如同下表所述。

表 3.256 終端機服務加密等級

加密等級	描述
高等級	此等級對由用戶端傳送到伺服器和伺服器到用戶端的資料，以強大的 128 位元加密法加密。當終端機伺服器執行於一個只包含 128 位元的用戶端（例如遠端桌面連線用戶端）環境時，使用此等級。不支援這種加密等級的用戶端將無法連線。
用戶端相容	此等級將用戶端和伺服器間傳送的資料，以用戶端所能支援的最大金鑰能力作加密。當終端機伺服器執行於一個包含混合或舊版用戶端的環境時，使用此等級。
低等級	此等級將用戶端傳送到伺服器的資料使用 56 位元的加密法加密。 重要：由伺服器傳送到用戶端的資料並未加密。

錯誤報告

表 3.257：設定值

UE 中的設定名稱	舊版用戶端	企業用戶端	高安全性	高安全性
NoNameReleaseOnDemand	DWORD	1	1	1

UE 中的設定名稱	舊版用戶端	企業用戶端	高安全性
報告錯誤	停用	停用	停用

Error Reporting (錯誤報告) 可協助 Microsoft 追蹤和解決錯誤。您可設定此服務來替作業系統錯誤、Windows 元件錯誤或程式錯誤產生報告。啟用 Report Errors 將會透過 Internet 將這類錯誤報告給 Microsoft，或報告給內部的公司檔案共用區。此設定只能用於 Windows XP Professional 和 Windows Server 2003。

設定此項設定的路徑位於「群組原則編輯器」中的：Computer Configuration\Administrative Templates\System>Error Reporting 內。

錯誤報告可能包含敏感、甚至機密的公司資料。Microsoft 關於錯誤報告的隱私權原則可確保 Microsoft 公司絕不會不當地使用該資料。不過這些資料是以純文字的 HTTP 來傳輸，因此可能會在 Internet 上被攔截，並被第三者所檢視。基於這些理由，此手冊建議您停用錯誤報告(Report Errors)。

摘要

本章說明了一開始套用至本手冊所定義三個安全性環境內所有伺服器的伺服器補強程序。這些程序中絕大多數的作法都是替每個安全性環境建立唯一的安全性範本，接著將它匯入到成員伺服器的父代 OU 所連結的 GPO 內，以取得目標的安全性等級。

不過，這些補強程序中有一些並無法透過群組原則來套用。此處針對了這些狀況，提供以手動方式設定這些補強程序的相關指示。特定的伺服器角色還會採取一些額外的步驟，讓它們儘可能安全地運作於它們的角色之中。

伺服器角色的相關步驟包括了額外的補強程序，以及在基礎安全性原則中減少安全性設定的程序。這些變更都將詳細地探討於本手冊後面的章節之中。

詳細資訊

底下的資訊來源列出了在本產品發行之際，與 Windows Server 2003 密切相關的最新主題。如需 Windows Server 2003 安全性設定描述的詳細資訊，請參閱：<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/615.asp>

如需 Windows Server 2003 安全性的詳細資訊，請參閱：http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_SEtopnode.asp.

如需 Windows Server 2003 稽核原則的詳細資訊，請參閱：<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/APtopnode.asp>.

如需 Microsoft Operations Manager (MOM) 的詳細資訊，請參閱：<http://www.microsoft.com/mom/>.

如需 Windows Server 2003 使用者權限設定的詳細資訊，請參閱：<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/URAtopnode.asp>.

如需 Windows Server 2003 預設安全性設定的詳細資訊，請參閱：
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/datacenter/windows_security_differences.asp.

如需保護 Windows 2000 終端機服務的詳細資訊，請參閱：<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/win2kts/maintain/optimize/secw2kts.asp>.

如需補強 Windows Server 2003 TCP/IP 堆疊的詳細資訊，請參閱 Microsoft 知識庫文章 Q324270 “Harden the TCP/IP Stack Against Denial of Service Attacks in Windows Server 2003”，網址為：
<http://support.microsoft.com/default.aspx?scid=324270>

如需補強 Windows Sockets 應用程式設定的詳細資訊，請參閱知識庫文章 Q142641 “Internet Server Unavailable Because of Malicious SYN Attacks”，網址為：
<http://support.microsoft.com/default.aspx?scid=142641>.

如需 .adm 檔位置的詳細資訊，請參閱知識庫文章 Q228460 “Location of ADM (Administrative Template) Files in Windows”，網址為：<http://support.microsoft.com/default.aspx?scid=228460>。

如需自訂 Security Configuration Editor 使用者介面的詳細資訊，請參閱 Microsoft 知識庫文章 214752 “How to Add Custom Registry Settings to Security Configuration Editor”，網址為：
<http://support.microsoft.com/default.aspx?scid=214752>。

如需在 Windows 中建立自訂管理範本檔的詳細資訊，請參閱知識庫文章 323639 “How to: Create Custom Administrative Templates in Windows 2000”，網址為：<http://support.microsoft.com/default.aspx?scid=323639>。此外，亦請參閱 “Implementing Registry-Based Group Policy” 白皮書，網址為：
<http://www.microsoft.com/WINDOWS2000/techinfo/howitworks/management/rbppaper.asp>。

如需替混用 Windows 2000 和 Windows NT 4.0 系統的網路提供更安全 LAN Manager Authentication Level 設定的詳細資訊，請參閱知識庫文章 Q305379 “Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain”，網址為：
<http://support.microsoft.com/default.aspx?scid=305379>。

如需 LAN Manager 相容性等級的詳細資訊，請參閱 <http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/regentry/76052.asp>。

如需 NTLMv2 驗證的詳細資訊，請參閱知識庫文章 Q239869，”How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT”，網址為：<http://support.microsoft.com/default.aspx?scid=239869>。

如需 Windows Server 2003 內服務的預設設定值的詳細資訊，請參閱：
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/datacenter/sys_srv_default_settings.asp。

如需智慧卡部署的詳細資訊，請參閱 Technet 智慧卡網站：
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/smrtdcard/default.asp>。

如需 Windows Server 2003 之稽核原則的詳細資訊，請參閱：<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/APtopnode.asp>。

如需 “RestrictAnonymous” 登錄值如何破壞對於 Windows 2000 網域之信任的詳細資訊，請參閱：
<http://support.microsoft.com/default.aspx?scid=kb;en-us;296405>。

如需停用錯誤報告的詳細資訊，請參閱：http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sysdm_advandcd_exception_reporting.asp。

如需 Windows Corporate Error Reporting 的詳細資訊，請參閱：
<http://www.microsoft.com/office/ork/xp/appndx/appa19.htm>。

4. 補強網域控制站

概觀

網域控制站伺服器角色，在保護任何執行 Microsoft® Windows Server 2003 並使用 Microsoft Active Directory® 目錄服務的電腦系統環境安全上，都扮演最重要的角色之一。系統環境中任何網域控制站的失敗或受侵害，都可能代表那些依賴網域控制站的驗證，群組原則，以及「集中式輕量型目錄存取通訊協定」(central lightweight directory access protocol，簡稱為 LDAP) 目錄的用戶端、伺服器、和應用程式的毀壞。

基於他們的重要性，網域控制站應該一直存放於最安全的位置，只能由合格的管理人員存取。當網域控制站一定要儲存在較不安全的地方時，例如分公司，則可以調整某些安全性設定，以減少駭客攻擊所帶來的潛在傷害。

網域控制站基礎原則

網域控制站伺服器角色的群組原則和本手冊中稍後會詳述的其他伺服器角色原則不同的是，它是一個基礎原則，其與第三章「建成立員伺服器基礎」所定義的「成員伺服器基礎原則」(MSBP) 同等級的。

「網域控制站基礎原則」(Domain Controllers Baseline Policy，簡稱為 DCBP) 連接到網域控制站組織單位(OU)，且優先次序凌駕於預設的網域控制站原則之上。在任何特定的環境中，DCBP 所包含的設定，能夠加強整個網域控制站的整體安全性。大多數 DCBP 是直接由 MSBP 複製而得。由於 DCBP 的基礎建立於 MSBP，因此，第三章「建成立員伺服器基礎」必需詳細閱讀，才能完全瞭解也包括在 DCBP 中的許多設定值。本章只記錄了與 MSBP 不同的 DCBP 的設定值。網域控制站範例，是針對本手冊所定義三個系統環境的安全性需求而特別設計的。下面這個表顯示了本手冊包括的網域控制站的 .inf 檔案，與這些環境間的關係。例如，Enterprise Client-Domain Controller.inf 檔案，是企業用戶端環境的安全性範例。

表 4.1：網域控制站基礎安全性範例

舊版用戶端	企業用戶端	高安全性
Legacy Client - Domain Controller.inf	Enterprise Client - Domain Controller.inf	High Security - Domain Controller.inf

注意：將設定錯誤的群組原則物件 (GPO) 連接到網域控制站 OU，可能會嚴重阻礙一個網域的正常運作。當匯入這些安全性範例時務必要格外小心，並且在把 GPO 連接到網域控制站 OU 之前，要確定所有匯入的設定值都是正確的。

稽核原則設定

網域控制站的稽核原則設定和 MSBP 中設定的那些是相同的。如需詳細資訊，請參閱第三章「建立成員伺服器基礎」。DCBP 的基礎原則設定，確保所有相關的安全性稽核資訊，都會登錄在網域控制站上。

使用者權限設定

DCBP 對網域控制站訂定了很多使用者權限設定。除了預設設定以外，另外也更改了七個使用者權限設定，以強化在本手冊所定義三個系統環境中網域控制站的安全性。

本節詳述了對 DCBP 的使用者權限設定所開立的處方，與 MSBP 不同之處。如需本節所定設定摘要，請參閱本手冊所附的 Windows Server 2003 Security Guide Settings Excel 工作簿。

由網路存取本電腦

表 4.2：設定值

網域控制站預設值	舊版用戶端	企業用戶端	高安全性
管理員，授權使用者，企業網域控制站 (ENTERPRISE DOMAIN CONTROLLERS)，每個人，與 Windows 2000 前相容的存取	未定義	未定義	管理員，授權使用者，企業網域控制站 (ENTERPRISE DOMAIN CONTROLLERS)

Access this computer from the network (由網路存取本電腦) 這使用者權限，決定了哪些使用者和群組被允許透過網路連接到本電腦。這項使用者權限是許多網路通訊協定所必需的，包括了以伺服器訊息區塊 (SMB) 為基礎的通訊協定、網路基本輸入輸出系統 (NetBIOS)、共同網際網路檔案系統 (CIFS)、Hypertext 傳輸通訊協定 (HTTP) 以及 Component Object Model Plus (COM+)。

雖然授權給 Everyone (每個人) 安全性群組的權限，不再授與存取權給 Windows Server 2003 中匿名使用者，但訪客(Guest)群組和帳戶仍可能透過 Everyone 安全性群組獲得存取權限。基於此項理由，本手冊建議在高安全性環境，從 Access this computer from the network 使用者權限移除 Everyone 安全性群組，以進一步防護企圖以訪客(Guest)存取網域的攻擊。

新增工作站到網域

表 4.3：設定值

網域控制站預設值	舊版用戶端	企業用戶端	高安全性
授權使用者	管理員	管理員	管理員

Add workstations to domain (新增工作站到網域) 使用者權限允許使用者新增電腦到特定網域。要使這權限發生作用，它必須指定給使用者，成為網域的「預設網域控制站原則」的一部份。擁有此權限的使用者可以新增至多 10 個工作站到網域。使用者獲得對 OU 或 Active Directory 的電腦容區(Computers

container) 的 Create Computer Objects (建立電腦物件) 權限，也可以加入電腦到網域。擁有此權限的使用者可新增無限多台電腦到網域，不論他們是否被指定「Add workstations to domain (新增工作站到網域)」。

預設狀態下，所有在 Authenticated Users (授權使用者) 群組的使用者都能新增至多 10 個電腦帳戶到 Active Directory 網域。這些新電腦帳戶是建立在電腦容區中。

在一個 Active Directory 網域，每一個電腦帳戶都是一個完整的安全性原則，能夠授權和存取網域資源。有些組織會想限制在一個 Active Directory 環境中電腦的數量，好使他們能對電腦作一致性地追蹤、建立和管理。

允許使用者把工作站加入網域會使這項工作受阻。因為他們可以建立額外的未授權的網域電腦，以致也提供了使用者管道去進行一些很難追蹤的活動。

基於這些理由，對本手冊中所定義的三個系統環境，「Add workstations to domain (新增工作站到網域)」使用者權限只有 Administrators(系統管理員)(系統管理員) 群組才能用。

允許本機登入

表 4.4：設定值

網域控制站預設值	舊版用戶端	企業用戶端	高安全性
管理員，帳戶操作員，備份操作員， 列印操作員，伺服器操作員	管理員	管理員	管理員

Allow log on locally (允許本機登入) 使用者權限可讓使用者在電腦上啟動互動式的工作。沒有這權限的使用者，如果擁有「Allow logon through Terminal Services (允許透過終端機服務登入)」權限，仍然能夠在電腦上啟動遠端的互動式工作。

限制用來登入系統環境的網域控制站主控台的帳戶，可預防未授權地存取網域控制站的檔案系統和系統服務。使用者若能登入網域控制站的主控台，可以惡意地利用系統，且很可能破壞整個網域或樹系的安全性。

在預設狀態下，Account Operators (帳戶操作員)、Backup Operators (備份操作員)、Print Operators (列印操作員) 和 Server Operators (伺服器操作員) 群組，都擁有登入網域控制站本機的權限。在這些群組的使用者卻不應該需要登入網域控制站執行他們的管理工作。這些群組的使用者，在正常狀況下可以由其他工作站執行他們日常的工作。只有 Administrators(系統管理員)(系統管理員) 群組使用者才應該在網域控制站上執行維護工作。

僅將此權限授與 Administrators(系統管理員)群組可將網域控制站的實際與互動地存取，限制於可高度信任的使用者，因此增進了安全性。基於此理由，本手冊所定義三個系統環境中，「Allow log on locally (允許本機登入)」使用者權限都僅授與 Administrators(系統管理員)(系統管理員)群組。

允許透過終端機服務登入

表 4.5：設定值

網域控制站預設值	舊版用戶端	企業用戶端	高安全性
未定義	管理員	管理員	管理員

Allow log on through Terminal Services (允許透過終端機服務登入) 使用者權限允許使用者藉由 Remote Desktop (遠端桌面) 連線登入電腦。

限制那些可以透過終端機服務登入系統環境的網域控制站主控台的帳戶，可有效預防未授權地存取網域控制站的檔案系統和系統服務。使用者若能透過終端機服務登入網域控制站的主控台，便可能惡意地利用系統，且很可能破壞整個網域或樹系的安全性。

僅將此權限授與 Administrators(系統管理員)群組可將網域控制站的互動式存取，限制於可高度信任的使用者，因此增進了安全性。基於此理由，本手冊所定義三個系統環境中，「Allow log on through Terminal Services (允許透過終端機服務登入)」使用者權限都僅授與 Administrators(系統管理員)群組。雖然透過終端機服務登入網域控制站，在預設狀態需要管理性的存取，但藉由設定此使用者權限，可幫助防護可能破壞此限制的不慎或惡意的動作。

為了更進一步的安全性考量，DCBP 不讓此權限預設的 Administrator 帳戶透過終端機服務登入網域控制站。這設定也防止惡意的使用者，使用預設的 Administrator 帳戶，企圖由遠端侵入網域控制站。如需這設定的詳細資訊，請參閱第三章「建立成員伺服器基礎」。

更改系統時間

表 4.6：設定值

網域控制站預設值	舊版用戶端	企業用戶端	高安全性
管理員，伺服器操作員	管理員	管理員	管理員

Change the system time (更改系統時間) 使用者權限允許使用者調整電腦內部的計時器。此權限對更改系統時間的時區或其他顯示特性是不需要的。

同步化的系統時間對 Active Directory 的運作來說相當重要。正確的 Active Directory 複寫和「Kerberos version 5 驗證通訊協定」所使用的驗證的憑證產生過程，都依賴整個環境具備同步化的時間。

網域控制站所設定的系統時間，如果和環境中其他網域控制站系統時間不同步，可能會干擾網域服務的運作。僅允許管理員能夠更改系統時間，使網域控制站被設定不正確的系統時間的可能性降到最低。

預設狀態下，Server Operators (伺服器操作員) 群組擁有更改網域控制站系統時間的權限。為了避免此群組的成員可能不正確地更改網域控制站的系統時間所造成的影響，對本手冊所定義三個系統環境，

DCBP 設定的這使用者權限，只有設定給 Administrators(系統管理員)群組。

如需 Microsoft Windows® 時間服務的詳細資訊，請參考知識庫文章 Q224799，”Basic Operation of the Windows Time Service”，其網址為：<http://support.microsoft.com/default.aspx?scid=224799>，以及 Q216734，”How to Configure an Authoritative Time Server in Windows 2000”，其網址為：<http://support.microsoft.com/default.aspx?scid=216734>。

啓用電腦和使用者帳戶被信任作委派

表 4.7：設定值

網域控制站預設值	舊版用戶端	企業用戶端	高安全性
管理員	未定義	未定義	管理員

Enable computer and user accounts to be trusted for delegation (啓用電腦和使用者帳戶被信任作委派) 使用者權限允許使用者更改 Active Directory 中使用者或電腦物件的「信任作委派」(Trusted for Delegation) 設定。驗證委派是多端點用戶端/伺服器應用程式所使用的一種功能。它允許前端服務能使用後端服務申請驗證的用戶端憑據。爲了達到此可能性，用戶端和伺服器二者都必須執行於能夠信任作委派的帳戶。

錯誤地使用此權限，可能導致未授權的使用者，能假冒網路上其他使用者的身份。駭客可以利用此權限，以另一個使用者身份出現，而得到網路資源的存取權，以致當發生安全性意外事件後，要辨讀出發生了什麼事會更加困難。

本手冊建議把「Enable computer and user accounts to be trusted for delegation (啓用電腦和使用者帳戶被信任作委派)」權限指定給網域控制站的 Administrators(系統管理員)群組。

注意：雖然預設網域控制站原則將此權限指定給 Administrators(系統管理員)群組，但 DCBP 只在高安全性環境加強此權限，因爲 DCBP 原本就是奠基於 MSBP，而 MSBP 的此權限是指定給 NULL 值。

載入和卸載裝置驅動程式

表 4.8：設定值

網域控制站預設值	舊版用戶端	企業用戶端	高安全性
管理員，列印操作員	管理員	管理員	管理員

Load and unload device drivers (載入和卸載裝置驅動程式) 使用者權限決定哪些使用者可以載入和卸載裝置驅動程式。此使用者權限對載入和卸載即插即用 (Plug and Play) 裝置是必需的。

惡意的載入或卸載網域控制站的裝置驅動程式，對其運作可能有極不利的影響。因此，必須限制只有最能信任的使用者帳戶，才能夠載入和卸載裝置驅動程式，使得利用裝置驅動程式破壞您環境中網域控制站的機會降到最低。

預設狀態下，Print Operators (列印操作員) 群組擁有此權限。如稍早所提，我們並不建議在網域控制站上建立印表機共用。這就移除了 Print Operators 要有此權限作載入和卸載裝置驅動程式的需求。因此，對本手冊所定義三個系統環境，此使用者權限都只授與 Administrators(系統管理員)群組。

復原檔案和目錄

表 4.9：設定值

網域控制站預設值	舊版用戶端	企業用戶端	高安全性
管理員，備份操作員， 伺服器操作員	管理員	管理員	管理員

Restore files and directories (復原檔案和目錄) 使用者權限允許使用者在復原備份檔案和目錄時，避開檔案和目錄權限，並設定任何合法的安全性原則作為物件的擁有者。

若讓使用者帳戶能夠復原網域控制站檔案系統的檔案和目錄，會使得該帳戶擁有者能夠輕易地更改服務執行檔。惡意的使用者不僅可以濫用這權限所提供的存取權，造成網域控制站變得毫無功用，還可能破壞網域或整個樹系的安全性。

預設狀態下，Server Operators (伺服器操作員) 和 Backup Operators (備份操作員) 群組擁有此權限。若移除這些群組的這個使用者權限，且只授權給 Administrators(系統管理員)(管理員) 群組，可降低對檔案系統不正確的修改、導致網域控制站被破壞的可能性。因此，本手冊中所定義三個系統環境中，此使用者權限都只授權給 Administrators(系統管理員)群組。

關閉系統

表 4.10：設定值

網域控制站預設值	舊版用戶端	企業用戶端	高安全性
管理員，伺服器操作員， 列印操作員，備份操作員	管理員	管理員	管理員

Shutdown the system (關閉系統) 使用者權限允許使用者把本機電腦關機。

惡意的使用者如果有能力關閉網域控制站，就能輕易地發動一個拒絕服務 (DoS) 的攻擊，使得整個網域和樹系受到嚴重影響。甚至，這使用者權限可能會被用來在網域控制站的系統帳戶重新啟動服務時，發動一個提高特權的攻擊。對網域控制站提高特權的攻擊若是成功，就危害到網域或整個樹系的安全性。

預設狀態下，Administrators、Server Operators、Print Operators 和 Backup Operators 群組都擁有將網域控制站關機的權限。在安全的環境中，這些群組除了 Administrators(系統管理員)以外，並不需要此權限來執行管理性工作。基於此理由，此使用者權限在本手冊所定義三個系統環境中，都只授權給 Administrators(系統管理員)群組。

安全性選項

大多數網域控制站的安全性選項設定和 MSBP 設定的相同。如需詳細資訊，請參閱第三章「建立成員伺服器基礎」。MSBP 與 DCBP 間的不同，將在以下這一節描述。

網路安全性：當下次密碼更改時，不要儲存 LAN Manager 雜湊值

表 4.11：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	啟用	啟用

Network Security: Do not store LAN Manager hash value on next password change (網路安全性：當下次密碼更改時，不要儲存 LAN Manager 雜湊值) 安全性選項設定決定 LAN Manager (LM) 當密碼更改時，是否儲存新密碼的雜湊值。LM 的雜湊法十分脆弱且易於受攻擊，相較之下 Windows NT® 的雜湊密碼學較強。基於此理由，MSBP 在本手冊定義的三個安全性系統環境中，將此設定設成啟用(Enabled)。

DCBP 中的這個設定，在企業用戶端和高安全性環境中的網域控制站是設成啟用，但在舊版用戶端環境的網域控制站則設成停用。若是在舊版用戶端環境中的網域控制站啟用此設定，Windows 98 用戶端在更改他們的密碼後，將無法登入。

注意：舊版作業系統和某些協力廠商的應用程式，在這設定啟用時，可能會失敗。還有，啟用此設定需要所有的帳戶都更改他們的密碼。

事件記錄檔設定

網域控制站的事件記錄檔 (Event Log) 設定和 MSBP 中設定的相同。如需詳細資訊，請參閱第三章「建立成員伺服器基礎」。在 DCBP 中的基礎群組原則設定，確保了所有相關的安全性稽核資訊都登錄到網域控制站上，包括了目錄服務存取。

系統服務

下面這些系統服務必須在所有 Windows Server 2003 網域控制站上啓用。DCBP 中的 基礎原則的設定可確保所有需要的系統服務都能夠在整個網域控制站中設定的一致性。

本節詳細說明與 MSBP 不同的 DCBP 的系統服務設定。如需本節所定的設定摘要，請參閱本手冊所附的 Windows Server 2003 Security Guide Settings Excel 工作簿。

注意：如果您從 Windows Server 2003 Support Tools 執行 DCDiag.exe 公用程式，它會檢查您環境中所有可以執行於網域控制站上的服務。DCDiag.exe 將會報告一些錯誤訊息，因為有些服務在網域控制站基礎原則中被停用了，其中包括了 IISADMIN、SMTPSVC 和 TrkSvr。這資訊並不代表您的設定有問題。

分散式檔案系統

表 4.12：設定值

網域控制站預設值	服務名稱	舊版用戶端	企業用戶端	高安全性
自動	Dfs	自動	自動	自動

Distributed File System (分散式檔案系統，簡稱為 DFS) 服務分配並整合不同類型的檔案共用，成為一個單一的邏輯名稱空間。此服務管理分佈於區域網路或廣域網路 (WAN) 的邏輯磁碟區，是 Active Directory 的系統磁碟區 (System Volume，簡稱為 SYSVOL) 共用所必需的。SYSVOL 的複寫依賴 DFS 的正確運作。

透過以群組原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器管理員，因此可防止未授權或惡意的使用者設定或操作該服務。群組原則也可防止管理員不慎地停用該服務。基於這些理由，本手冊所定義的三個系統環境中，DCBP 把這服務設定成自動(Automatic)。

DNS 伺服器

表 4.13：設定值

網域控制站預設值	服務名稱	舊版用戶端	企業用戶端	高安全性
自動	Dns	自動	自動	自動

DNS Server (DNS 伺服器) 服務解析「網域名稱系統」(Domain Name System，簡稱為 DNS) 查詢和更新 DNS 名稱的需求。DNS Server 是一項重要的服務，用來找出那些在 Active Directory 中以 DNS 名稱和網域控制站作識別的裝置位於何處。

Active Directory 的可靠性和可用性來自於 DNS Server 服務的能否正確運作。少了 DNS，網域控制站便無法找出彼此位置以複寫目錄資訊，而用戶端也不能連繫到網域控制站作驗證。

透過以群組原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器管理員，因此可防止未授

權或惡意的使用者設定或操作該服務。群組原則也可防止管理員不慎地停用該服務。基於這些理由，本手冊所定義的三個系統環境中，DCBP 把這服務設定成自動(Automatic)。

檔案複寫

表 4.14：設定值

網域控制站預設值	服務名稱	舊版用戶端	企業用戶端	高安全性
自動	NtFrs	自動	自動	自動

File Replication (檔案複寫) 服務可讓檔案同時自動地複製，並在多重伺服器上進行維護作業。檔案複寫服務 (簡稱為 FRS) 是在 Windows 2000 和 Windows Server 家族中，檔案自動複寫的服務。這服務複寫所有網域控制站上的 SYSVOL，並且可以設定成複寫與容錯 DFS 相關連的其他目的地檔案。SYSVOL 複寫也依賴 File Replication 服務的正确運作。

透過以群組原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器管理員，因此可防止未授權或惡意的使用者設定或操作該服務。群組原則也可防止管理員不慎地停用此服務。基於這些理由，在本手冊所定義三個系統環境中，DCBP 的這服務是設定成自動(Automatic)。

網站間訊息傳輸

表 4.15：設定值

網域控制站預設值	服務名稱	舊版用戶端	企業用戶端	高安全性
自動	IsmServ	自動	自動	自動

Intersite Messaging (網站間訊息傳輸，簡稱為 ISM) 服務使執行 Windows 伺服器網站的電腦間能互相交換訊息。這服務用來作網站間以郵件為基礎的複寫。Active Directory 包括了支援網站間經由「網際網路通訊協定」(IP) 傳輸、使用「簡單郵件傳輸通訊協定」(SMTP) 的複寫。SMTP 支援是由 SMTP 服務這 Microsoft 網際網路資訊服務 (IIS) 的元件所提供的。

用來在網站間通訊的傳輸集合必須有延展性；因此，每一個傳輸是定義成一個獨立可加入的 DLL (dynamic link library)。這些新加入的 DLL 被載入 ISM 服務後，此服務會在所有可能會進行網站間通訊的網域控制站上執行。ISM 服務會將傳送和接收訊息需求轉向到適當的傳輸DLL增益集，然後把訊息遞送到目標電腦的 ISM 服務。Active Directory 複寫須仰賴 Intersite Messaging 服務的正确執行。

透過以群組原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器管理員，因此可防止未授權或惡意的使用者設定或操作該服務。群組原則也可防止管理員不慎地停用該服務。基於這些理由，在本手冊所定義三個系統環境中，DCBP 的這服務是設定成自動(Automatic)。

Kerberos 金鑰發行中心

表 4.16：設定值

網域控制站預設值	服務名稱	舊版用戶端	企業用戶端	高安全性
自動	Kdc	自動	自動	自動

Kerberos Key Distribution Center (金鑰發行中心，簡稱為 KDC) 服務讓使用者能用 Kerberos v5 驗證通訊協定登入網路。

KDC 服務是使用者登入網路所必需的。停用此服務 使用者將無法登入網路。

透過以群組原則來保護與設定服務的起動模式，系統可將存取權只授與伺服器管理員，藉此來防止未授權或惡意的使用者設定或操作該服務。群組原則也可防止管理員不慎地停用該服務。基於這些理由，在本手冊所定義三個系統環境中，DCBP 的這服務是設定成自動(Automatic)。

遠端程序呼叫定位器

表 4.17：設定值

網域控制站預設值	服務名稱	舊版用戶端	企業用戶端	高安全性
自動	RpcLocator	自動	自動	自動

Remote Procedure Call (RPC) Locator (遠端程序呼叫定位器) 服務讓 RPC 用戶端能利用 RpcNs* 家族的 API (application programming interfaces) 來尋找 RPC 伺服器，並管理 RPC 名稱服務資料庫。

停止或停用此服務會使得使用 RpcNs* API 的 RPC 用戶端找不到伺服器或是起動失敗。此外，同一台電腦上依賴 RpcNs* API 的 RPC 用戶端，可能會找不到支援某個特定介面的 RPC 伺服器。停止或停用您網域控制站的這服務，會使得使用 RpcNs* API 的 RPC 用戶端和網域控制站，在試著去找用戶端時，遭遇服務中斷的問題。

透過以群組原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器管理員，因此可防止未授權或惡意的使用者設定或操作該服務。群組原則也可防止管理員不慎地停用該服務。基於這些理由，在本手冊所定義三個系統環境中，DCBP 的這服務是設定成自動(Automatic)。

其他安全性設定

本節描述了必須對 DCBP 所作手動的更改，以及無法經由群組原則實作的其他設定與對策。

手動地將唯一的安全性群組加至使用者權限設定內

大多數經由 DCBP 套用的使用者權限設定 (User Rights Assignments) 都在本手冊所附的安全性範本指定範圍內。不過，仍有一些帳戶和安全性群組無法納入範本之中，因為其安全性識別項 (SID) 僅適用於個別的 Windows 2003 網域。必須手動設定的使用者權限設定列出如下。

警告：下表包含了內建 Administrator 帳戶的值。請勿將此帳戶和內建的 Administrators(系統管理員)安全性群組搞混了。若 Administrators (系統管理員)安全性群組已加至底下的任一個拒絕存取使用者權限中，您需要登入於本機來訂正此錯誤。此外，內建的 Administrators(系統管理員)帳戶可能已根據第三章「建立成員伺服器基礎」所述的一些建議重新命名。在加入 Administrator 帳戶時，請記得指定重新命名的帳戶。

表 4.18：手動加入使用者權限設定

網域控制站預設值	舊版用戶端	企業用戶端	高安全性
拒絕經由網路存取此電腦	內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶	內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶	內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶
拒絕以批次工作登入	Support_388945a0 和 Guest	Support_388945a0 和 Guest	Support_388945a0 和 Guest
拒絕經由終端機服務登入	內建管理員; 所有非作業 系統服務的帳戶	內建管理員; 所有非作業 系統服務的帳戶	內建管理員; 所有非作業 系統服務的帳戶

重要：所有非作業系統服務的帳戶包括了企業內特定應用程式所使用的服務帳戶。這並未包含 LOCAL SYSTEM、LOCAL SERVICE 或 NETWORK SERVICE 帳戶，它們都是作業系統使用的內建帳戶。

目錄服務

執行 Windows Server 2003 的網域控制站主要是用來儲存目錄資料、管理使用者和網域之互動，包括使用者登入過程、驗證和目錄搜尋。

更換資料位置 — Active Directory 資料庫和記錄檔

保護 Active Directory 資料庫和記錄檔的安全，對維護目錄完整性和可靠性是相當重要的。

把 `ntds.dit`、`edb.log` 和 `temp.edb` 檔案從他們的預設位置搬移，能讓網域控制站在受攻擊時，從駭客前將他們隱藏起來。此外，把檔案從系統磁碟區搬到另一個實體分開的磁碟，也能增進網域控制站效能。

基於這些理由，在本手冊所定義三個系統環境中，我們建議把 Active Directory 網域控制站的資料庫和記錄檔，從他們系統磁碟區的預設位置搬移到一個非系統等量 (non-system striped) 或等量/鏡像 (striped/mirrored) 的磁碟區。

改變 Active Directory 記錄檔大小

確保整個環境的網域控制站具備足夠數量的資訊記錄和維護，對有效地監視與維護 Active Directory 的完整性、可靠性和可用性來說是非常重要的。

增加記錄檔大小的最大容量，能幫助系統管理員保有足夠的資訊來以支援稽核駭客攻擊的事件。

基於這些理由，本手冊建議在本手冊所定義三個系統環境的網域控制站上，把目錄服務和檔案複寫服務的記錄檔大小最大容量，由 512 KB 預設值改為 16 MB。

使用 Syskey

在網域控制站上，密碼資訊是儲存於目錄服務中。密碼竊取軟體以「安全性帳戶管理員」(Security Account Manager，簡稱爲 SAM) 資料庫或目錄服務爲目標，存取使用者帳戶密碼也時有所聞。

System Key (Syskey) 公用程式對離線的密碼竊取軟體提供額外一道防護。Syskey 使用強大的加密技術保護存於目錄服務的帳戶密碼資訊。

表 4.19：Syskey 模式

SysKey 選項	安全等級	描述
模式 1：系統產生密碼、儲存起動金鑰於本機	安全	使用電腦產生的亂數金鑰作為系統的金鑰，並儲存加密版本的金鑰於本機電腦。此選項提供記錄中的密碼資訊強大的加密，且能讓使用者不必管理員輸入密碼或插入磁片就能重新起動電腦。
模式 2：管理員產生密碼、起動密碼	較安全	使用電腦產生的亂數金鑰作為系統的金鑰，並儲存加密版本的金鑰於本機電腦。這金鑰同時也由管理員所選定的金鑰密碼所保護。當電腦在起始的起動順序中，使用者會被提示要求系統金鑰密碼。系統金鑰密碼並不儲存在電腦上任何地方。
模式 3：系統產生密碼、儲存起動金鑰於磁片	最安全	使用電腦產生的亂數金鑰並把金鑰儲存於磁片上。系統起動時，這片含有系統金鑰的磁片是必需的，在起動順序中會有提示要求插入它。系統金鑰密碼並不儲存在電腦上任何地方。

所有的 Windows Server 2003 伺服器中，Syskey 都是啓用在模式 1 (混亂金鑰)。有很多原因，對於任何暴露於實際的安全性攻擊之網域控制站，我們建議使用 Syskey 於模式 2 (主控台密碼) 或模式 3 (儲存 Syskey 密碼於磁片)。

首先，從安全性的觀點，這顯得很敏感，因為網域控制站可能很容易被可實際存取它的駭客重新起動。Syskey 模式 1 允許駭客讀取並更改目錄的內容。

然而，為確保網域控制站能透過重新起動而能夠運作的操作需求，使得支援 Syskey 模式 2 或模式 3 變得很困難。為了善加利用這些 Syskey 模式所提供的額外保護，您的系統環境必須導入正確的操作過程，以滿足網域控制站特定的可用性需求。

Syskey 密碼或磁片管理的後勤作業可能很複雜，特別是在分公司。例如，需要您分公司管理員或本機管理員工在清晨 3 點到達公司輸入密碼或插入磁片、讓使用者能存取系統的這代價很昂貴，且使要達到高可用性的服務等級 (SLA) 十分具挑戰性。

另一選擇，允許您集中式的 IT 運作人員在遠端提供 Syskey 密碼需要額外的硬體；有些硬體廠商可提供增加性的解決方案，從遠端存取伺服器主控台。

最後，Syskey 密碼或磁片的遺失將造成您的網域控制站處在一個不能起動的狀態。假使 Syskey 密碼或磁片遺失的話，您沒有方法修復網域控制站。萬一發生這種情形，網域控制站必須重新建立。

雖然如此，但是靠著正確的運作程序，Syskey 能提供高等級的安全性，可大大保護網域控制站上敏感的目錄資訊。

基於這些理由，對不處於堅固且實際安全的儲存地方的網域控制站，我們建議用 Syskey 模式 2 或模式 3。這建議也適用於任何本手冊所描述三種環境中的網域控制站。

- 建立或更新系統金鑰：

1. 按一下 Start (開始)，點選 Run (執行)，輸入 syskey，然後點選 OK (確定)。
2. 點選 Encryption Enabled (啓用加密)，然後點選 Update (更新)。
3. 點選所想要的選項，然後點選 OK (確定)。

Active Directory 整合式 DNS

Microsoft 建議本手冊在所定義三個系統環境中，使用 Active Directory 整合式 DNS，部分原因是因為整合區域到 Active Directory 可簡化保護 DNS 基礎架構的流程。

保護 DNS 伺服器

在任何 Active Directory 環境中保護 DNS 伺服器都是很重要的。下面的幾節提供了一些建議並解釋了這樣做的原因。

當 DNS 伺服器受到攻擊，駭客的可能目標之一，就是想控制 DNS 對其用戶端查詢所回應的資訊。在這樣的情況下，用戶端可能會不慎地被轉向到未授權的電腦。IP 欺騙 (IP spoofing) 和快取區下毒 (cache poisoning) 就是這種型態攻擊的例子。

IP 欺騙傳輸特定授權使用者 IP 位址以得到電腦或網路存取權。快取區下毒這種攻擊則是未授權的主機傳遞有關另一台主機的錯誤資訊到 DNS 伺服器的快取區。這種攻擊會造成用戶端被指向與未授權的電腦通訊。

一旦用戶端不慎地開始與未授權的電腦通訊，那些電腦可能企圖得到儲存於用戶端電腦的存取資訊。

並非所有的攻擊重心都透過欺騙 DNS 伺服器。一些 DoS 攻擊可能改變合法 DNS 伺服器中的 DNS 記錄，對用戶端的查詢提供不合法的位址。藉著使伺服器以不合法的位址來回應，用戶端和伺服器將無法找到他們所需功能的資源，例如網域控制站、Web 伺服器或檔案共用。

基於這些理由，本手冊建議在這三個系統環境所使用的路由器，設定成去掉欺騙的 IP 封包，以確保 DNS 伺服器的 IP 位址不會被其他電腦欺騙。

設定安全動態更新

Windows Server 2003 DNS 用戶端服務支援動態 DNS 更新，能允許用戶端系統直接在資料庫中新增 DNS 記錄。如果伺服器設定成接受不安全的更新，動態 DNS 伺服器可能會收到惡意的或未授權的更新，這是由駭客所使用支援 DDNS 通訊協定的用戶端所發出。

最輕微情況，駭客可新增假造的項目到 DNS 資料庫；最糟情況下，駭客可以覆寫或刪除 DNS 資料庫中合法的項目。這種攻擊可能造成任何以下的情況：

- 用戶端被指向未授權的網域控制站：當一用戶端發出 DNS 查詢，尋找一個網域控制站的位址時，受侵害的 DNS 伺服器可被指示傳回未授權伺服器的位址。然後，駭客會利用其他非 DNS 相關的去進行攻擊，而用戶端可能因此被騙，而把安全資訊傳給這台假冒的伺服器。
- 以不合法的位址回應 DNS 的查詢：這使得用戶端和伺服器無法找到彼此。如果用戶端找不到伺服器，他們就無法存取目錄。當網域控制站找不到其他網域控制站，目錄複寫便會停擺，並產生一個 DoS 事件，這很可能影響到整個樹系的使用者。
- 創造一個 DoS 狀況，使得其中一台伺服器的磁碟空間，充滿了巨大區域檔案無用的記錄，或一大堆項目使空間耗盡且複寫變慢。

安全的 DDNS 更新可保證只處理 Active Directory 樹系中合法的用戶端所傳送出的登錄需求。這可大大地限制駭客破壞 DNS 伺服器完整性的機會。

基於這些理由，本手冊建議，對手冊所定義三個系統環境的 Active Directory DNS 伺服器，設定成只接受安全動態更新 (Secure Dynamic Updates)。

限制區域傳輸給授權的系統

由於區域 (zone) 在 DNS 中所扮演的重要角色，他們應可從網路上不只一台 DNS 伺服器使用，以提供足夠的可用性和容錯性來解析名稱查詢。否則，只傳送給區域中一台伺服器的名稱查詢如果沒有得到反應，可能會導致解析失敗。其他的伺服器要掛接於一區域，區域傳輸需要複寫和同步化所有設定成掛接到這區域的每台伺服器所使用的區域備份。

此外，DNS 伺服器如果不設定成對要求區域傳輸的人作限制，將很容易傳輸整個 DNS 區域給任何要求它的人。用像 nslookup.exe 這種工具很容易達成這情況。這種工具可以暴露整個網域的 DNS 資料集合，包括了哪些作為網域控制站服務的主機，目錄整合的 Web 伺服器，或是 Microsoft SQL Server 2000 資料庫。

基於這些理由，本手冊建議在本手冊所定義三個系統環境中，設定 Active Directory 整合的 DNS 伺服器，允許區域傳輸，但可傳輸的系統必須受到限制。

改變事件記錄檔和 DNS 服務記錄檔大小

確保環境中的網域控制站有足夠多的資訊記錄及維護，對有效地監視 DNS 服務是很重要的。增加 DNS 服務記錄檔的最大容量能幫助管理員維護足夠多的資訊，在駭客攻擊的事件中實行有意義的稽核。

基於此理由，本手冊建議，對本手冊所定義三個系統環境中，網域控制站 DNS 服務記錄檔的最大容量設定成至少 16 MB，並確保 DNS 服務中的 Overwrite events as needed (有需要時覆寫事件) 選項被勾選，使保留記錄項目有最大容量。

保護知名帳戶

Windows Server 2003 擁有許多內建使用者帳戶，是無法刪除但可重新命名的。Windows 2003 內兩個最有名的內建帳戶為 Guest 與 Administrator。

在預設狀態下，Guest 帳戶在成員伺服器 and 網域控制站上 are 停用的。此設定不應該變更。內建的 Administrator 帳戶應該重新命名，而描述也應改變，以防止駭客使用知名的帳戶危害遠端的伺服器。

許多惡意程式碼的變型都在初次嘗試中使用內建的管理員帳戶來危害伺服器。近年來，變更這項組態所可帶來的價值已逐漸減少，因為現在嘗試侵入伺服器的攻擊工具會指定內建 Administrator 帳戶的 SID 來決定其真正的名稱。SID 指的是可唯一識別網路上每個使用者、群組、電腦帳戶和登入工作階段的數值。您不可能變更此內建帳戶的 SID。將本機管理員帳戶重新命名為唯一的名稱，可讓您的作業群組監視嘗試攻擊此帳戶的事件。

請照以下步驟完成對網域和伺服器上知名帳戶的保護：

1. 在每個網域和伺服器上，重新命名 Administrator 和 Guest 帳戶，並將其密碼變更為長而複雜的值。
2. 在伺服器上使用不同的名稱和密碼。若所有的網域和伺服器上都使用相同的帳戶名稱和密碼，則可存取某台成員伺服器的駭客，即可以相同的帳戶名稱和密碼來存取所有其他的伺服器。
3. 將帳戶描述變更為預設值以外的值，以防止他人輕易地識別出帳戶。
4. 將這些變更記錄在安全的位置。

注意：內建的 Administrator 帳戶可透過群組原則來重新命名。在 DCBP 中並未設定此項設定，因為您必須為您的環境選擇一個獨特的名稱。您可設定 Accounts：Rename administrator account 設定值，以便將此手冊所定義三個系統環境中的管理員帳戶重新命名。此設定值是 GPO 的安全性選項設定的一部份。

保護服務帳戶

除非絕對必要，否則千萬不要將服務設定成在網域帳戶的安全性內容底下執行。若伺服器已實體地受到危害，他人即可透過傾印 Local Security Authority (本機的安全性授權單位，簡稱為LSA) 秘密，輕鬆取得網域帳戶的密碼。

終端機服務設定

表 4.20：設定值

預設值	舊版用戶端	企業用戶端	高安全性
設定用戶端連線加密等級	高	高	高

Set client connection encryption level (設定用戶端連線加密等級) 這設定可決定您環境中終端機服務用戶端連線的加密等級。**High Level (高等級)** 設定選項使用 128 位元加密來防止駭客在終端機服務期間使用封包分析程式偷聽。一些較舊版本的終端機服務用戶端並不支援這種高等級的加密。如果您的網路含有這種用戶端，要將傳送和接收資料的加密等級，則在用戶端設定支援最高的加密等級。基於這些理由，本手冊建議在本手冊所定義三個系統環境中的 DCBP，將「Set client connection encryption level (設定用戶端連線加密等級)」設定成 Enabled (啟用)，並選擇 High Level (高等級) 加密選項。

設定此項設定的路徑在「群組原則物件編輯器」中的：
Computer Configuration\Administrative Templates\Windows
Components\Terminal Services\Encryption and Security

有三種加密等級可用：

表 4.21：終端機服務加密等級

加密等級	描述
高等級	此等級對由用戶端傳送到伺服器 and 伺服器到用戶端的資料，以強大的 128 位元加密法加密。當終端機伺服器執行於一個只包含 128 位元的用戶端（例如遠端桌面連線用戶端）環境時，使用此等級。不支援這種加密等級的用戶端將無法連線。
用戶端相容	此等級將用戶端和伺服器間傳送的資料，以用戶端所能支援的最大金鑰能力作加密。當終端機伺服器執行於一個包含混合或舊版用戶端的環境時，使用此等級。
低等級	此等級將用戶端傳送到伺服器的資料使用 56 位元的加密法加密。 重要：由伺服器傳送到用戶端的資料並未加密。

錯誤報告

表 4.22：設定值

預設值	舊版用戶端	企業用戶端	高安全性
報告錯誤	停用	停用	停用

Error Reporting (錯誤報告) 服務可協助微軟追蹤和解決錯誤。您可設定此服務來產生作業系統錯誤、Windows 元件錯誤或程式錯誤的報告。啟用 Report Errors 服務將會透過 Internet 將這類錯誤報告給微軟，或傳送至公司內部檔案共用區中。

此設定只能用於 Microsoft Windows® XP Professional 和 Windows Server 2003。在「群組原則 物件編輯器」中設定此設定值的路徑為：

Computer Configuration\Administrative Templates\System>Error Reporting

錯誤報告可能包含敏感、甚至機密的公司資料。微軟關於錯誤報告的隱私權原則可確保微軟不至於不當地使用這類資料，不過由於資料是以純文字 Hypertext Transfer Protocol (HTTP) 來傳送，它可能會在 Internet 上遭到攔截，並被協力廠商所檢視。基於這些理由，在本手冊所定義的三個安全性環境中，本手冊都建議您在 DCP 中將 Error Reporting 設定值設成 Disabled (停用)。

以 IPSec 篩選器封鎖連接埠

Internet Protocol Security (IPSec) 篩選器可提供有效的方法來增強伺服器所需的安全性等級。此手冊替手冊內所定義的高安全性環境建議此選擇性指引，以進一步地減少伺服器的攻擊面。

如需使用 IPSec 篩選器的詳細資訊，請參閱下列隨附手冊的第 11 章「Additional Member Server Hardening Procedures」：《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》。

下表列出了所有應該建立於本手冊所定義高安全性環境之網域控制站的 IPSec 篩選器。

表 4.23：網域控制站 IPSec 篩選器網路傳輸對應

服務	通訊協定	來源連接埠	目標連接埠	來源位址	目標位址	動作	鏡像
CIFS/SMB 伺服器	TCP	AN	445	任意	ME	允許	是
	UDP	任意	445	任意	ME	允許	是
RPC 伺服器	TCP	任意	135	任意	ME	允許	是
	UDP	任意	135	任意	ME	允許	是
NetBIOS 伺服器	TCP	任意	137	任意	ME	允許	是
	UDP	任意	137	任意	ME	允許	是
	UDP	任意	138	任意	ME	允許	是
	TCP	任意	139	任意	ME	允許	是
監視用戶端	任意	任意	任意	ME	MOM 伺服器	允許	是
終端機服務伺服器	TCP	任意	3389	任意	ME	允許	是
Global Catalog 伺服器	TCP	任意	3268	任意	ME	允許	是
	TCP	任意	3269	任意	ME	允許	是

服務	通訊協定	來源連接埠	目標連接埠	來源位址	目標位址	動作	鏡像
DNS 伺服器	TCP	任意	53	任意	ME	允許	是
	UDP	任意	53	任意	ME	允許	是
Kerberos 伺服器	TCP	任意	88	任意	ME	允許	是
	UDP	任意	88	任意	ME	允許	是
LDAP 伺服器	TCP	任意	389	任意	ME	允許	是
	UDP	任意	389	任意	ME	允許	是
	TCP	任意	636	任意	ME	允許	是
	UDP	任意	636	任意	ME	允許	是
NTP 伺服器	TCP	任意	123	任意	ME	允許	是
	UDP	任意	123	任意	ME	允許	是
靜態 AD 複寫伺服器	TCP	任意	57952	任意	ME	允許	是
DC Comms	任意	任意	任意	ME	網域控制站	允許	是
DC Comms	任意	任意	任意	ME	網域控制站 2	允許	是
ICMP	ICMP	任意	任意	ME	任意	允許	是
所有傳入的傳輸資料	任意	任意	任意	任意	ME	封鎖	是

上表所列的所有規則都應在實作時加以鏡像。這可確保傳入伺服器內的任何網路傳輸資料亦可回到原本的伺服器中。

上表代表了應開啓哪些基底連接埠，以便讓伺服器執行其特定角色的功能。若伺服器擁有靜態的 IP 位址，這些連接埠就已足夠。若要提供額外的功能，可能還需要開啓額外的連接埠。

開啓額外的連接埠可讓您環境中的網域控制站較易管理，不過，它們可能會大大降低這些伺服器的安全性。

從知識庫文章 Q224196 來的建議：“Restricting Active Directory Replication Traffic to a Specific Port”，其網址為 <http://support.microsoft.com/default.aspx?scid=224196>，需要實作於網域控制站。這能確保對特定連接埠會作網域複寫。

再次強調，針對此目的您應該使用超過 50,000 的亂數連接埠。在上面的例子，便是使用連接埠 57952。在您環境中應該使用不同的連接埠，而這項變更應在這指引導入的所有網域控制站執行。在實作這知識庫文章的步驟後，伺服器必須重新起動變更才會生效。

如上所示地，若 Microsoft Operations Manager (MOM) 實作於環境中，所有的網路傳輸資料都必須能夠在實作 IPSec 篩選器的伺服器 and MOM 伺服器之間傳送。因為 MOM 伺服器和 OnePoint 用戶端 (向 MOM 主控台報告的用戶端應用程式) 之間有大量的互動，所以這是有必要的。其他管理套件可能擁有類似的需求。若需要更大的安全性，您可設定 OnePoint 用戶端進行篩選動作以使得 IPSec 與 MOM 伺服器能夠相互協調。

IPSec 原則可透過隨機的高連接埠有效地封鎖傳輸量，並藉此禁止遠端程序呼叫 (RPC) 的傳輸。這會使得伺服器的管理變得相當困難。因為這些連接埠都已經有效地關閉，終端機服務也被啓用。如此可讓系統管理員去執行遠端系統管理。

上述的網路傳輸對應是假設環境中包含了具備 Active Directory 能力的 DNS 伺服器。若使用獨立的 DNS 伺服器，可能還需要額外的規則。

實作 IPSec 原則應不至於對伺服器的效能造成嚴重影響。不過，您仍應在實作這些篩選器之前進行測試，以確保伺服器的必要功能和效能都可維持。您可能也需要加入額外的規則來支援其他應用程式。

注意：網域控制站是非常動態的，因此在其上實作 IPSec 篩選器應該要小心評估，然後在實驗室環境中作整體測試。由於網域控制站間的大量互動，IPSec 篩選器加入時，必須允許彼此複寫資訊的網域控制站間的所有傳輸。在很多台網域控制站的複雜環境中，這將需要建立很多個額外的篩選器，使篩選器可以有效地保護網域控制站。這可能會令 IPSec 原則的實作和管理變得極為困難。但是，網域控制站少的環境，可以有效地利用到實作 IPSec 篩選器得到的好處。

本手冊有提供一個 .cmd 檔，其可簡化建立適用於網域控制站的 IPSec 篩選器的工作。PacketFilters-DC.cmd 檔使用 NETSH 命令來建立適當的篩選器。這個 .cmd 檔必須修改，以包含環境中其他網域控制站的 IP 位址。其指令碼包含了可加入兩個網域控制站的預留位置。若有需要，可將額外的網域控制站加至指令碼內。網域控制站的 IP 位址清單必須保持在最新狀態。

若 MOM 出現在環境之中，適當 MOM 伺服器的 IP 位址也必須指定於指令碼內。此指令碼並不會建立永續性篩選器。因此，伺服器需等到 IPSec Policy Agent 啟動時才會受到保護。如需建立永續性篩選器或建立更進階 IPSec 篩選器指令碼的詳細資訊，請參閱下列所附手冊的第 11 章「Additional Member Server Hardening Procedures」：《Threats and Countermeasures：Security Settings in Windows Server 2003 and Windows XP》。最後，此指令碼已設定成不指定它建立的 IPSec 原則。IP Security Policy Management 嵌入式管理單元可用來檢查建立的 IPSec 篩選器，並指定 IPSec 原則，以便讓它生效。

摘要

本章說明了伺服器的補強設定，以保護本手冊所定義三個系統環境中，每個系統環境的網域控制站。大多數我們所討論的設定是套用使用群組原則來做設定的。群組原則物件 (GPO) 是設計用來補足連結至網域控制站組織單位 (OU) 的「預設網域控制站原則」。「網域控制站基礎原則」(DCBP) 所包含的設定，將在任何給定的環境中，增強整個網域控制站的整體安全性。使用兩個 GPO 來保護網域控制站能夠保存預設環境並簡化疑難排解。

有一些伺服器補強設定不能透過群組原則套用。針對這些狀況，我們提供了以手動方式設定這些設定值的詳細資訊。

現在網域控制站可說已被安全地保護，本手冊下面的各章焦點將放在保護其他特定的伺服器角色。

詳細資訊

底下的資訊來源列出了在本產品發行之際，與執行 Windows Server 2003 的電腦所在環境中的網域控制站密切相關的最新主題。

如需 Microsoft 系統架構企業 Data Center 規範性架構手冊的相關資訊，請參閱：

<http://www.microsoft.com/technet/itsolutions/edc/default.asp>.

如需對 Active Directory 啟用匿名存取的相關資訊，請參閱知識庫文章 257988，”Description of Dcpromo Permissions Choices”，網址為：<http://support.microsoft.com/default.aspx?scid=257988>.

如需 Windows 2000 DNS 的相關資訊，請參閱“Windows 2000 DNS White Paper”，網址為：

<http://www.microsoft.com/windows2000/techinfo/howitworks/communications/nameadmgmt/w2kdns.asp>.

如需 Windows 2000 DNS 的詳細資訊，請參閱“TCP/IP Core Networking Guide”線上版本的第六章，網址為：

<http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp>.

如需 Windows 2003 DNS 相關資訊，請參閱“Changes to DNS in Windows Server 2003”，網址為：

<http://www.microsoft.com/windows2000/technologies/communications/dns/dns2003.asp>。

如需 IPsec 篩選器詳細資訊，請參閱“How To: Use IPsec IP Filter Lists in Windows 2000”，網址為：

<http://support.microsoft.com/default.aspx?scid=313190>.

如需限制 Active Directory 的詳細資訊，請參閱“Restricting Active Directory Replication Traffic to a Specific Port”，網址為：<http://support.microsoft.com/default.aspx?scid=224196>.

如需限制 FRS 複寫傳輸的詳細資訊，請參閱“How to Restrict FRS Replication Traffic to a Specific Static Port”，網址為：<http://support.microsoft.com/default.aspx?scid=319553>.

如需 Windows 時間服務的詳細資訊，請參閱“Basic Operation of the Windows Time Service”，網址為：

<http://support.microsoft.com/default.aspx?scid=224799>.

如需設定 Windows 時間服務的詳細資訊，請參閱“How to Configure an Authoritative Time Server in Windows 2000”，網址為：<http://support.microsoft.com/default.aspx?scid=216734>.

如需 IP 欺騙的詳細資訊，請參閱 SANS Info Sec Reading Room 中的文章，網址為：

http://www.sans.org/rr/threats/intro_spoofing.php.

5. 補強基礎架構伺服器

概觀

本章說明了伺服器的補強設定，以保護本手冊所定義的三個系統環境中的基礎架構伺服器。就本手冊的用途而言，基礎架構伺服器指的是提供 Dynamic Host Control Protocol (DHCP) 服務或 Microsoft® Windows® Internet Name Service (WINS) 功能的伺服器。

大多數所討論的設定都是套用群組原則來進行設定的。群組原則物件 (GPO) 主要是設計用來補足可連結至包含基礎架構伺服器的適當組織單位 (OU) 的成員伺服器基礎原則 (Member Server Baseline Policy，簡寫為 MSBP)，並依據這些伺服器所提供的服務，提供額外的安全性。

一些討論的設定並不能使用群組原則來套用。針對這些狀況，本章將提供以手動方式設定這些設定值的細節。此外，此處也提供建立與套用 Internet Protocol Security (IPSec) 篩選器的細節，以控制可與本章所述兩類基礎架構伺服器進行通訊的網路傳輸類型。

為改善本章的可用性，此處只包含了以 MSBP 修改的設定。如需 MSBP 內設定的相關資訊，請參閱第三章「建立成員伺服器基礎」。如需所有預設值的相關資訊，請參閱所附的手冊，《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》。

稽核原則設定

本手冊所定義三個系統環境中的基礎架構伺服器的稽核原則 (Audit Policy) 設定都是透過 MSBP 來設定。如需 MSBP 的詳細資訊，請參閱第三章「建成立員伺服器基礎」。MSBP 設定可確保所有相關的安全性稽核資訊都記錄在所有的基礎架構伺服器上。

使用者權限設定

本手冊所定義三個系統環境中的基礎架構伺服器的使用者權限設定 (User Rights Assignments) 都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建成立員伺服器基礎」。MSBP 設定可確保所有適當的使用者權限設定都一致地在所有的基礎架構伺服器上設定。

安全性選項

本手冊所定義三個系統環境中的基礎架構伺服器的安全性選項 (Security Options) 設定都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建成立員伺服器基礎」。MSBP 設定可確保所有相關的安全性選項都一致地在所有的基礎架構伺服器上設定。

事件記錄檔設定

本手冊所定義三個系統環境中的基礎架構伺服器的事件記錄檔 (Event Log) 設定都是透過 MSBP 來設定。如需 MSBP 的詳細資訊，請參閱第三章「建成立員伺服器基礎」。

系統服務

此「系統服務設定」小節提供了應將您系統環境中的基礎架構伺服器上的預定系統啓用或停用的詳細資訊。

這些服務設定都在基礎架構伺服器累加原則 (Infrastructure Server Incremental Policy) 內有定義。爲了將拒絕服務 (DoS) 攻擊的可能性降至最低，GPO 會確保這些服務都設成自動啓動。如需本章節的預設值設定摘要，請參閱本手冊所附的 Windows Server 2003 Security Guide Settings Excel 工作簿。

DHCP Server

表 5.1：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
DHCP	未安裝	自動	自動	自動

DHCP 服務會自動配置 Internet Protocol (IP) 位址，並啓用進階的網路設定組態 (例如 DNS 伺服器和 WINS 伺服器) 給 DHCP 用戶端。DHCP 使用了用戶端/伺服器模型。網路管理員建立了一個或多個 DHCP 伺服器來維護 Transmission Control Protocol/Internet Protocol (TCP/IP) 組態資訊，並將它提供給用戶端。

DHCP Server 服務必須持續執行，如此 DHCP 伺服器才能指定 IP 位址組態給其用戶端。透過以群組原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器管理員，因此可防止未授權或惡意的使用者設定或操作該服務。群組原則也可防止管理員不慎地停用該服務。

WINS

表 5.2：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
WINS	未安裝	自動	自動	自動

WINS 啓用了網路基本輸入/輸出系統 (NetBIOS) 名稱解析。WINS 伺服器是否存在，對於尋找以 NetBIOS 名稱來辨識的網路資源相當重要。除非所有網域都升級至 Microsoft Active Directory®、網路上所有的電腦都執行 Windows 2000 (含) 以後版本、並且沒有應用程式倚賴 WINS 解析來進行適當的操作，否則 WINS 伺服器是必要的。

WINS Server 服務必須持續執行，WINS 伺服器才能提供名稱解析給其用戶端。透過以群組原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器管理員，因此可防止未授權或惡意的使用者設定或操作該服務。群組原則也可防止管理員不慎地停用該服務。

其他安全性設定

透過 MSBP 套用的安全性設定，也提供基礎架構伺服器許多增強的安全性。但還有一些額外的事項需要考慮。這些步驟並無法透過群組原則來完成，並應手動地執行於所有的基礎架構伺服器上。

設定 DHCP 記錄

在預設狀態下，DHCP 服務只會在 Event Viewer 中記錄啟動和關閉的事件。

- 您可使用下列步驟，在 DHCP 伺服器上啟用更詳細的記錄：
 1. 以滑鼠右鍵在 DHCP 管理工具中按一下 DHCP 伺服器。
 2. 選取 Properties。
 3. 在 Properties 對話方塊的 General 標引標籤內，按一下 Enable DHCP Audit Logging。

完成這些步驟之後，DHCP 伺服器將在下列位置中建立一個記錄檔：

`%systemroot%\system32\dhcp\`

DHCP 用戶端通常很難找到記錄檔項目，因為儲存於大多數事件記錄檔內的資訊都只有電腦名稱，而沒有 IP 位址。DHCP 稽核記錄檔可多提供一個工具，讓您找出內部攻擊或疏忽活動的來源。

不過，這些記錄檔內的資訊並無法防止他人搗亂，因為不管是主機名稱和媒體存取控制 (MAC) 位址都可以偽造或欺騙。欺騙指的是讓傳輸看起來好像來自某個使用者，而非真正執行動作的使用者。不過，收集此資訊的好處大大超越在 DHCP 伺服器上啟用記錄所需的成本。擁有多個 IP 位址和機器名稱，將有助於決定特定的 IP 位址如何用於網路上。

Server Operators (伺服器操作員) 和 Authenticated Users (驗證使用者) 在預設狀態下，將擁有這些記錄檔的讀取權限。為了妥善地保存 DHCP 伺服器所記錄資訊的完整性，建議您只讓伺服器管理員存取這些記錄檔。

Server Operators 和 Authenticated Users 群組應從 `%systemroot%\system32\dhcp\` 資料夾的存取控制清單 (Access Control List，簡寫為 ACL) 中移除。

理論上，DHCP 稽核記錄檔可填滿它們所在的磁碟。不過，DHCP 稽核記錄設定的預設組態會確保此記錄動作將在伺服器上的可用磁碟空間少於 20 MB 時停止。此預設設定對於大多數環境的伺服器已綽綽有餘，但您亦可修改此設定，確保伺服器上的其他應用程式都有足夠的可用磁碟空間可用。如需修改此設定的相關資訊，請參閱 Windows 2000 Server Resource Kit 的「DhcpLogMinSpaceOnDisk」主題，網址為：
<http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/regentry/46692.asp>。

本文件所描述的登錄設定也適用於執行於 Windows Server 2003 上的 DHCP。

防止 DHCP 的拒絕服務攻擊

因為 DHCP 伺服器是讓用戶端存取網路的重要資源，它們可能成為 DoS 攻擊的主要目標。若 DHCP 伺服器受到攻擊，並且無法再服務 DHCP 要求，DHCP 用戶端最後將無法取得使用期 (Lease)。之後這些用戶端將會遺失其現有的 IP 使用期，以及存取網路資源的能力。

要編寫一個攻擊工具指令碼來要求 DHCP 伺服器上所有可用的位址並不困難。其可耗盡可用的 IP 位址集區，導致接下來的 DHCP 用戶端做合法要求，也沒有 IP 可用。惡意的使用者也可能設定所管理電腦的網路介面卡上的所有 DHCP IP 位址，因而令 DHCP 伺服器偵測其範圍內所有位址的 IP 位址衝突，並拒絕配置 DHCP 使用期。

再者，就和所有其他的網路服務一樣，其會令 DHCP 伺服器無法回應合法傳輸的 DoS 攻擊 – 例如，CPU 耗盡或填滿 DHCP 接聽項的要求緩衝區 – 可能令用戶端無法要求使用期和更新。透過妥善地設計環境中的 DHCP 服務，即可避免這些問題。

若能夠對地設定 DHCP 伺服器，並遵循最佳實施方針 80/20 規則 – 也就是分割伺服器的 DHCP 伺服器範圍，則一台 DHCP 伺服器便可分配 80% 的位址，另外 20 % 則由另一台來分配 – 確保伺服器發生故障時，用戶端仍可持續地接收 IP 位址組態，並因而降低這類攻擊所帶來的負面影響。如需 80/20 規則和 DHCP 通訊協定的詳細資訊，請參閱 Windows 2000 Server Resource Kit 內的 DHCP 通訊協定主題，網址為：http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/cnet/cncb_dhc_ogjw.asp。

保護知名帳戶

Windows Server 2003 擁有許多無法刪除、但可重新命名的內建使用者帳戶。Windows 2003 內兩個最有名的內建帳戶為 Guest 與 Administrator。

在成員伺服器和網域控制站上，是將 Guest 帳戶預設為停用。此設定不應該變更。而內建的 Administrator 帳戶則應該重新命名，而描述也應改變，以防止攻擊者使用知名的帳戶去危害遠端的伺服器。

許多惡意程式碼的變態都是在初次嘗試中使用內建的管理員帳戶來危害伺服器。近年來，自從嘗試侵入伺服器的攻擊工具會指定內建 Administrator 帳戶的安全性識別項 (SID) 來決定其真正的名稱後，變更這項組態變更的價值便逐漸減少。SID 指的是可唯一識別網路上每個使用者、群組、電腦帳戶和登入工作階段的數值。您不可能變更此內建帳戶的 SID。若將本機管理員帳戶重新命名成唯一的名稱，可讓您的作業群組監視嘗試攻擊此帳戶的事件。

- 要保護基礎架構伺服器上的知名帳戶：

1. 在每個網域和伺服器上，重新命名 Administrator 和 Guest 帳戶，然後將其密碼變更為長而複雜的值。
2. 在伺服器上使用不同的名稱和密碼。若所有的網域和伺服器上都使用相同的帳戶名稱和密碼，那麼可存取某台成員伺服器的攻擊者即可以相同的帳戶名稱和密碼來存取所有其他的伺服器。
3. 將帳戶描述變更為預設值以外的值，以防止他人輕易地識別出帳戶。
4. 將這些變更記錄在安全的位置。

注意：內建的 Administrator 帳戶可透過群組原則來重新命名。此設定值並未設定於本手冊所提供的任何安全性範本內，因為您應替您的環境選擇唯一的名稱。您可設定 Accounts:Rename administrator account 設定值，以便將此手冊所定義三個系統環境中的管理員帳戶全都重新命名。此設定值是安全性選項設定值 GPO 的一部份。

保護服務帳戶

除非必要，否則千萬不要將服務設定成執行於網域帳戶的安全性內容底下。若伺服器已實體地受到危害，他人即可透過傾印 Local Security Authority (LSA) 秘密，輕鬆取得網域帳戶的密碼。

以 IPSec 篩選器封鎖連接埠

Internet Protocol Security (IPSec) 篩選器可提供有效的方法來增強伺服器所需的安全性等級。此手冊替手冊內所定義的高安全性環境建議此選擇性指引，以進一步地減少伺服器的攻擊面。

如需使用 IPSec 篩選器的詳細資訊，請參閱下列隨附手冊的第 11 章，"Additional Member Server Hardening Procedures"：《Threats and Countermeasures:Security Settings in Windows Server 2003 and Windows XP》。

下表列出了所有可建立於本手冊所定義高安全性環境之 DHCP 伺服器上的 IPsec 篩選器。

表 5.3：DHCP 伺服器 IPsec 網路傳輸對應

服務	通訊協定	來源連接埠	目標連接埠	來源位址	目標位址	動作	鏡像
OnePoint 用戶端	任意	任意	任意	ME	MOM Server	允許	是
終端機服務	TCP	任意	3389	任意	ME	允許	是
網域成員	任意	任意	任意	ME	網域控制站	允許	是
網域成員	任意	任意	任意	ME	網域控制站 2	允許	是
DHCP 伺服器	UDP	68	67	任意	ME	允許	是
所有傳入的傳輸資料	任意	任意	任意	任意	ME	封鎖	是

下表列出了所有可建立於本手冊所定義高安全性環境之 WINS 伺服器上的 IPsec 篩選器。

表 5.4：WINS 伺服器 IPsec 網路傳輸對應

服務	通訊協定	來源連接埠	目標連接埠	來源位址	目標位址	動作	鏡像
OnePoint 用戶端	任意	任意	任意	ME	MOM Server	允許	是
終端機服務	TCP	任意	3389	任意	ME	允許	是
網域成員	任意	任意	任意	ME	網域控制站	允許	是
網域成員	任意	任意	任意	ME	網域控制站 2	允許	是
WINS 解析伺服器	TCP	任意	1512	任意	ME	允許	是
	UDP	任意	1512	任意	ME	允許	是
WINS 複寫用戶端	TCP	任意	42	ME	WINS 複寫協 力電腦	允許	是
	UDP	任意	42	ME	WINS 複寫協 力電腦	允許	是
WINS 複寫伺服器	TCP	任意	42	WINS 複寫協 力電腦	ME	允許	是
	UDP	任意	42	WINS 複寫協 力電腦	ME	允許	是
所有傳入的傳輸資料	任意	任意	任意	任意	ME	封鎖	是

上表所列的所有規則都應在實作時加以鏡像。這可確保傳入伺服器內的任何網路傳輸資料亦可回到原本的伺服器中。

上表說明哪些基底連接埠需要開啓，以便讓伺服器執行其角色的相關功能。若伺服器擁有靜態的 IP 位址，這些連接埠就已足夠。若要提供額外的功能，可能還需要開啓額外的連接埠。開啓額外的連接埠可讓您環境中的基礎架構伺服器更容易管理，不過，它們可能會大大降低這些伺服器的安全性。

因為網域成員和網域控制站之間有大量的互動，特別是 RPC 和驗證傳輸，所有的通訊都允許傳輸於基礎架構伺服器和所有的網域控制站之間。其實它們之間的傳輸是可以進一步做限制，但是大多數的環境都需要額外建立數十個篩選器，才能讓篩選器有效地保護伺服器。這可能會令 IPSec 原則的實作和管理變得極為困難。因為與基礎架構伺服器互動的每個網域控制站都需建立類似的規則。若想要增加基礎架構伺服器的可靠性和可用性，則需另外在您系統環境的所有網域控制站中增加規則。

如上所示地，若 Microsoft Operations Manager (MOM) 實作於環境中，所有的網路傳輸資料都必須可傳送至實作 IPSec 篩選器的伺服器和 MOM 伺服器之間。因為 MOM 伺服器和 OnePoint 用戶端 (向 MOM 主控台報告的用戶端應用程式) 之間有大量的互動，這是必要的。其他管理套件可能擁有類似的需求。若需要更大的安全性，您可設定 OnePoint 用戶端的篩選器動作，以便與 MOM 伺服器協商 IPSec 的相關議題。

這項 IPSec 原則可透過隨機的高連接埠來有效封鎖傳輸量，藉此禁止遠端程序呼叫 (RPC) 的傳輸。這將令伺服器的管理變得困難。因為已有這麼多的連接埠被有效地關閉，終端機服務也被啓用。這可讓管理員執行遠端管理。

上述的網路傳輸對應將假設環境中包含了具備 Active Directory 能力的 DNS 伺服器。若使用獨立的 DNS 伺服器，可能還需要額外的規則。

實作 IPSec 原則基本上不會嚴重地影響伺服器的效能。不過，您仍應在實作這些篩選器之前進行測試，以確保伺服器的必要功能和效能都可維持。而您也有可能需要加入額外的規則來支援其他應用程式。

本手冊包含了一些 .cmd 檔，可讓您更輕鬆地建立適用基礎架構伺服器的 IPSec 篩選器。PacketFilters-DHCP.cmd 和 PacketFilters-WINS.cmd 檔都使用 NETSH 命令來建立適當的篩選器。您必須修改這些 .cmd 檔，才能夠包含您系統環境中的網域控制站的 IP 位址。指令碼包含了預留位置以供兩個網域控制站的新增。若有需要，您可將另外增加網域控制站到這些指令碼內。此外，網域控制站的 IP 位址清單必須保持在最新狀態。這裡面還加入了僅適用 WINS 複寫協力電腦的預留位置。適當的 WINS 複寫協力電腦也必須指定於 PacketFilters-WINS.cmd 檔內，如此 WINS 複寫才會生效。

若 MOM 出現在環境之中，適當 MOM 伺服器的 IP 位址也必須在指令碼內指定。此指令碼並不會建立永續性篩選器。因此，伺服器需等到 IPSec Policy Agent 啟動時才會受到保護。如需建立永續性篩選器或建立更進階 IPSec 篩選器指令碼的詳細資訊，請參閱下列所附手冊的第 11 章「Additional Member Server Hardening Procedures」：《Threats and Countermeasures:Security Settings in Windows Server 2003 and Windows XP》。最後，此指令碼已設定成不指定它建立的 IPSec 原則。IP Security Policy Management 嵌入式管理單元可用來檢查建立的 IPSec 篩選器，並指定 IPSec 原則，以便讓它生效。

摘要

本章說明了伺服器補強設定，以保護本手冊所定義三個系統環境中的 DHCP 和 WINS 伺服器。這些角色的大多數設定都是透過 MSBP 來套用。DHCP 和 WINS 伺服器的累加 .inf 檔的主要目標是讓這些角色的必要服務完整地作用，同時又確保其安全性。

雖然 MSBP 提供極高的安全性，此處仍探討了基礎架構角色的一些其他考量。這些考量主要包含了啟用記錄和選擇性地使用 IPSec 篩選器來封鎖傳給這些電腦的未授權網路傳輸資料。

詳細資訊

底下的資訊來源列出了在本產品發行之際，與執行 Windows Server 2003 的電腦所在環境中的基礎架構伺服器密切相關的最新主題。

如需 Windows Server 2003 對 DHCP 記錄所做變更的最新資訊，請參閱：

<http://support.microsoft.com/default.aspx?scid=328891>.

如需 Active Directory 網域內 DHCP 伺服器的詳細資訊，請參閱“[How To: Install and Configure a DHCP Server in an Active Directory Domain in Windows Server 2003](#)”，網址為：

<http://support.microsoft.com/default.aspx?scid=323360>.

如需 DHCP 的詳細資訊，請參閱：

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/reskit/tcpip/part2/tcpch04.asp>

如需 WINS 的詳細資訊，請參閱：

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/evaluate/featfunc/nt5wins.asp>.

如需在 Windows Server 2003 中安裝 Wins 的相關資訊，請參閱“[How To: Install WINS in Windows Server 2003](#)”，網址為：<http://support.microsoft.com/default.aspx?scid=323429>.

6. 補強檔案伺服器

概觀

若您想要進一步地補強檔案伺服器，您將會碰到一些挑戰，因為它們提供的最基本服務是需要 Microsoft® Windows® Network Basic Input/Output System (NetBIOS) 相關通訊協定的服務。Server Message Block (SMB) 和 Common Internet File System (CIFS) 的通訊協定可提供豐富的資訊給未經驗證的使用者。因此，您最好不要讓檔案伺服器在高安全性的 Windows 環境中使用這些通訊協定。不過，若停用這些通訊協定，不管是環境中的管理員或使用者，都會很難存取檔案伺服器。

本章的底下章節將詳細地說明檔案伺服器可在哪些領域中從非 Member Server Baseline Policy (MSBP) 所套用的安全性設定中獲益。如需 MSBP 的詳細資訊，請參閱第三章「建成立員伺服器基礎」。

稽核原則設定

本手冊所定義三個環境中的檔案伺服器的稽核原則 (Audit Policy) 設定都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建成立員伺服器基礎」。MSBP 設定可確保所有相關的安全性稽核資訊都記錄於所有的檔案伺服器上。

使用者權限指定

本手冊所定義三個環境中的檔案伺服器的使用者權限設定 (User Rights Assignments) 都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建成立員伺服器基礎」。MSBP 設定可確保所有適當的使用者權限設定都一致地設定於所有的檔案伺服器上。

安全性選項

本手冊所定義三個環境中的檔案伺服器的安全性選項 (Security Options) 設定都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建成立員伺服器基礎」。MSBP 設定可確保所有相關的安全性選項都一致地設定於所有的檔案伺服器上。

事件記錄檔設定

本手冊所定義三個環境中的檔案伺服器的事件記錄檔 (Event Log) 設定都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建成立員伺服器基礎」。

系統服務

任何服務或應用程式都是一個潛在的攻擊弱點，因此任何沒有必要的服務或執行檔都應停止使用或移除。在 MSBP 中，選擇性的服務以及任何沒有必要的服務都會停用。

執行 Microsoft Windows Server™ 2003 的檔案伺服器上通常所啓用的某些額外服務並不是必要的。這些服務的用途和安全性經常成為爭議的焦點。基於此理由，本手冊對於檔案伺服器的建議未必適用於您的系統環境。請依需要調整檔案伺服器群組原則的建議，以符合您組織的需求。

分散式檔案系統：

表 6.1：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
DFS	自動	停用	停用	停用

Distributed File System (分散式檔案系統，簡寫為 DFS) 服務管理了分散於區域網路 (LAN) 或廣域網路 (WAN) 上的邏輯磁碟區，並且必須用於 Microsoft Active Directory® SYSVOL 共用區。DFS 是一個分散式服務，可將不同的檔案共用區整合到單一的邏輯命名空間內。

此命名空間是可供網路上使用者運用的網路儲存資源的邏輯表示。停用 DFS 服務可防止使用者透過邏輯命名空間來存取網路資料，並且要求他們需知道環境中所有伺服器和共用區的名稱，方能存取它們。

檔案伺服器累加群組原則 (File Server Incremental Group Policy) 會停用 DFS 服務，以便將您環境內檔案伺服器的攻擊面減至最少。基於此理由，「Distributed File System (分散式檔案系統)」設定值在本手冊所定義的所有安全性環境中都設成 停用(Disabled)。

注意：對於在檔案伺服器上以 DFS 來簡化分散式資源之存取的組織而言，它們必須修改檔案伺服器累加群組原則或建立新的 GPO，方能啓用此服務。

檔案複寫服務

表 6.2：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
NTFRS	手動	停用	停用	停用

File Replication Service (檔案複寫服務，簡寫為 FRS) 可在多重伺服器上自動複製檔案及維護檔案。FRS 為 Windows® 2000 和 Windows Server 的自動化檔案複寫服務。2003 family。此服務會在所有的網域控制站上複寫系統磁碟區 (Sysvol)。此外，此服務也可設定成在容錯 DFS 的相關替換目標間複寫檔案。若此服務為停用，便不會發生檔案複寫，而伺服器資料也不會同步化。

檔案伺服器累加群組原則將令 FRS 無法將您環境之檔案伺服器的攻擊面降至最低。基於此理由，「File Replication Service (檔案複寫服務)」設定值在本手冊所定義的所有安全性環境中都應設成 停用 (Disabled)。

注意：對於在檔案伺服器上以 FRS 在多重伺服器之間複寫資料的組織而言，它們必須修改檔案伺服器累加群組原則或建立新的 GPO，方能啟用此服務。

其他安全性設定

透過 MSBP 套用的安全性設定替檔案伺服器提供了許多增強的安全性。但還有一些額外的事項需要考慮。這些步驟並無法透過群組原則來完成，並應手動地執行於所有的檔案伺服器上。

保護知名帳戶

Microsoft Windows Server™ 2003 擁有許多無法刪除、但可重新命名的內建使用者帳戶。Windows 2003 內兩個最有名的內建帳戶為 Guest 與 Administrator。

Guest 帳戶在預設狀態下在成員伺服器和網域控制站上是設成停用。此設定不應該變更。內建的 Administrator 帳戶應該重新命名，而描述也應改變，以防止攻擊者使用知名的帳戶危害遠端的伺服器。

許多惡意程式碼的變型都在初次嘗試中使用內建的管理員帳戶來危害伺服器。近年來，此組態變更的價值已逐漸減少，因為現在嘗試侵入伺服器的攻擊工具會指定內建 Administrator 帳戶的安全性識別項 (SID) 來決定其真正的名稱。SID 指的是可唯一識別網路上每個使用者、群組、電腦帳戶和登入工作階段的數值。您不可能變更此內建帳戶的 SID。將本機管理員帳戶重新命名為唯一的名稱，可讓您的作業群組監視嘗試攻擊此帳戶的事件。

- 要保護檔案伺服器上的知名帳戶：
 1. 在每個網域和伺服器上，重新命名 Administrator 和 Guest 帳戶，然後將其密碼變更為長而複雜的值。
 2. 在伺服器上使用不同的名稱和密碼。若所有的網域和伺服器上都使用相同的帳戶名稱和密碼，那麼可存取某台成員伺服器的攻擊者即可以相同的帳戶名稱和密碼來存取所有其他的伺服器。
 3. 將帳戶描述變更為預設值以外的值，以防止他人輕易地識別出帳戶。
 4. 將這些變更記錄在安全的位置。

注意：內建的 Administrator 帳戶可透過群組原則來重新命名。此設定值並未設定於本手冊所提供的任何安全性範本內，因為您應替您的環境選擇唯一的名稱。您可設定 Accounts:Rename administrator account 設定值，以便將此手冊所定義三個環境中的管理員帳戶全都重新命名。在群組原則中，此設定值是安全性選項設定值的一部份。

保護服務帳戶

除非必要，否則千萬不要將服務設定成在網域帳戶的安全性內容底下執行。若伺服器已實體地受到危害，他人即可透過傾印 Local Security Authority (LSA) 秘密，輕鬆取得網域帳戶的密碼。

以 IPSec 篩選器封鎖連接埠

Internet Protocol Security (IPSec) 篩選器可提供有效的方法來增強伺服器所需的安全性等級。此手冊替手冊內所定義的高安全性環境建議此選擇性指引，以進一步地減少伺服器的攻擊面。

如需使用 IPSec 篩選器的詳細資訊，請參閱下列隨附手冊的第 11 章，「Additional Member Server Hardening Procedures」：《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》。

下表列出了所有可建立於本手冊所定義高安全性環境之檔案伺服器上的 IPSec 篩選器。

表 6.3：DHCP 伺服器 IPSec 網路傳輸對應

服務	通訊協定	來源連接埠	目標連接埠	來源位址	目標位址	動作	鏡像
CIFS Server	TCP	任意	445	任意	ME	允許	是
	UDP	任意	445	任意	ME	允許	是
NetBIOS Server	TCP	任意	137	任意	ME	允許	是
	UDP	任意	137	任意	ME	允許	是
	UDP	任意	138	任意	ME	允許	是
	TCP	任意	139	任意	ME	允許	是
OnePoint 用戶端	任意	任意	任意	ME	MOM Server	允許	是
終端機服務	TCP	任意	3389	任意	ME	允許	是
網域成員	任意	任意	任意	ME	網域控制站	允許	是
網域成員	任意	任意	任意	ME	網域控制站 2	允許	是
所有傳入的傳輸資料	任意	任意	任意	任意	ME	封鎖	是

上表所列的所有規則都應在實作時加以鏡像。這可確保傳入伺服器內的任何網路傳輸資料亦可回到原本的伺服器中。

上表代表了應開啓哪些基底連接埠，以便讓伺服器執行其角色的相關功能。若伺服器擁有靜態的 IP 位址，這些連接埠就已足夠。若要提供額外的功能，可能還需要另外開啓其他的連接埠。雖然開啓額外的連接埠可讓您環境中的檔案伺服器更容易管理，不過，也可能會大大降低這些伺服器的安全性。

因為網域成員和網域控制站之間有大量的互動，特別是 RPC 和驗證傳輸，所有的通訊都允許傳輸於檔案伺服器 and 所有的網域控制站之間。事實上，可以進一步限制它們之間的傳輸，但是大多數的環境都需要額外建立數十個篩選器，才能讓篩選器有效地保護伺服器。這可能會令 IPSec 原則的實作和管理變得極為困難。因為與檔案伺服器互動的每個網域控制站都需建立類似的規則。若想要增加檔案伺服器的可靠性和可用性，則需另外在您系統環境的所有網域控制站中增加規則。

如上所示地，若 Microsoft Operations Manager (MOM) 實作於環境中，所有的網路傳輸資料都必須可傳送於實作 IPSec 篩選器的伺服器和 MOM 伺服器之間。因為 MOM 伺服器和 OnePoint 用戶端 (向 MOM 主控台報告的用戶端應用程式) 之間有大量的互動，這是必要的。其他管理套件可能擁有類似的需求。若需要更大的安全性，您可設定 OnePoint 用戶端的篩選器動作，以便與 MOM 伺服器協商 IPSec 的相關議題。

此 IPSec 原則可透過隨機的高連接埠有效地封鎖傳輸，藉此禁止遠端程序呼叫 (RPC) 的傳輸。這將令伺服器的管理變得困難。因為這麼多的連接埠已經有效地關閉，終端機服務將被啟用。這可讓管理員執行遠端管理。

上述的網路傳輸對應將假設環境中包含了具備 Active Directory 能力的 DNS 伺服器。若使用獨立的 DNS 伺服器，可能還需要額外的規則。

實作 IPSec 原則基本上不會嚴重地影響伺服器的效能。不過，您仍應在實作這些篩選器之前進行測試，以確保伺服器的必要功能和效能都可維持。而您也有可能需要加入額外的規則來支援其他應用程式。

本手冊包含了一個 .cmd 檔，可讓您更輕鬆地建立適用檔案伺服器的 IPSec 篩選器。PacketFilters-File.cmd 檔使用 NETSH 命令來建立適當的篩選器。您必須修改此 .cmd 檔，以包含您環境之網域控制站的 IP 位址。指令碼包含了預留位置來加入兩個網域控制站。若有需要，可再加入額外的網域控制站。網域控制站的 IP 位址清單必須保持在最新狀態。

若 MOM 出現在環境之中，適當 MOM 伺服器的 IP 位址也必須指定於指令碼內。此指令碼並不會建立永續性篩選器。因此，伺服器需等到 IPSec Policy Agent 啟動時才會受到保護。如需建立永續性篩選器或建立更進階 IPSec 篩選器指令碼的詳細資訊，請參閱下列所附手冊的第 11 章「Additional Member Server Hardening Procedures」：《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》。最後，此指令碼已設定成不指定它建立的 IPSec 原則。IP Security Policy Management 嵌入式管理單元可用來檢查建立的 IPSec 篩選器，並指定 IPSec 原則，以便讓它生效。

摘要

本章說明了伺服器的補強設定，以保護本手冊所定義三個系統環境中的檔案伺服器。大多數所討論的設定都是使用群組原則來設定與套用的。群組原則物件 (GPO) 是設計用來補足連結至網域控制站組織單位 (OU) 的「預設網域控制站原則」。「網域控制站基礎原則」(DCBP) 所包含的設定，將在任何給定的環境中，增強整個網域控制站的整體安全性。

某些討論的設定並不能使用群組原則來套用。針對這些狀況，本章提供了手動設定這些設定值的細節。此外，本章也提供建立與套用 IPSec 篩選器的細節，以控制可與檔案伺服器進行通訊的網路傳輸類型。

詳細資訊

底下的資訊來源列出了在本產品發行之際，與執行 Windows Server 2003 的電腦所在環境中的檔案伺服器密切相關的最新主題。

如需檔案伺服器的詳細資訊，請參閱“Technical Overview of Windows Server 2003 File Services”，網址為：
<http://www.microsoft.com/windowsserver2003/techinfo/overview/file.mspx>。

如需 DFS 的詳細資訊，請參閱“Distributed File System”白皮書，網址為：
<http://www.microsoft.com/windows2000/techinfo/howitworks/fileandprint/dfsnew.asp>。

如需 FRS 的詳細資訊，請參閱“File Replication Service”，網址為：
http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/distrib/dsdh_frfs_BNYR.asp。

如需 IPSec 篩選的詳細資訊，請參閱“How To: Use IPSec IP Filter Lists in Windows 2000”，網址為：
<http://support.microsoft.com/default.aspx?scid=313190>。

7. 補強列印伺服器

概觀

本章的重點在於更進一步補強列印伺服器所可能面臨的挑戰，因為他們所提供的最基本的服務，需要 Microsoft® Windows® 網路基本輸入輸出系統 (NetBIOS) 相關的通訊協定。Server Message Block (伺服器訊息區塊，簡稱為 SMB) 和 Common Internet File System (共同網際網路檔案系統，簡稱為 CIFS) 通訊協定，可提供給未驗證的使用者豐富的資訊，因此在高安全性的 Windows® 環境中，通常建議列印伺服器停用這些通訊協定。然而，停用這些通訊協定，將可能造成您環境中不論是管理員或使用者，存取伺服器上的困難。

本章中其他各節將詳細地說明列印伺服器可在哪些領域中從非 Member Server Baseline Policy (MSBP) 所套用的安全性設定中獲益。如需 MSBP 的詳細資訊，請參閱第三章「建成立員伺服器基礎」。

稽核原則設定

本手冊所定義三個系統環境中的列印伺服器的稽核原則 (Audit Policy) 設定都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建立成員伺服器基礎」。MSBP 設定可確保所有相關的安全性稽核資訊都記錄於所有的列印伺服器上。

使用者權限指定

本手冊所定義三個系統環境中的列印伺服器的使用者權限設定 (User Rights Assignments) 都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建立成員伺服器基礎」。MSBP 設定可確保所有適當的使用者權限設定，都一致地設定於所有的列印伺服器上。

安全性選項

本手冊所定義三個系統環境中的列印伺服器的安全性選項 (Security Options) 設定，大多數都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建成立員伺服器基礎」。MSBP 與 Incremental IIS 群組原則之間的不同，將在以下這一節描述。

Microsoft 網路伺服器：數位簽章通訊（永遠）

表 7.1：設定值

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
停用	停用	停用	停用

Microsoft network server：Digitally sign communications (always) (數位簽章通訊（永遠）) 設定值可決定 SMB 伺服器元件是否需要封包簽章。SMB 通訊協定提供基礎給 Microsoft 檔案與列印共用，以及很多其他網路作業，例如遠端的 Windows 管理。爲了防止在傳輸中有人中途攻擊並更改 SMB 封包，SMB 通訊協定可支援 SMB 封包數位簽章。這個設定值會決定在允許與 SMB 用戶端作更進一步通訊前，SMB 封包簽章是否必須先經過協商。

雖然這個設定值的預設值是停用的，但 MSBP 爲在本手冊定義的高安全性環境中的伺服器，啓用了這個設定值。列印伺服器上的這設定值若未被停用，就表示允許使用者列印，但不能檢視列印佇列。企圖檢視列印佇列的使用者，將會收到一個存取被拒絕的訊息。基於這些原因，「Microsoft network server：Digitally sign communications (always) (數位簽章通訊（永遠）)」設定值在本手冊所定義三個系統環境中，對列印伺服器都是設定成停用的。

事件記錄檔設定

本手冊所定義三個系統環境中的列印伺服器之事件記錄檔 (Event Log) 設定都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建成立員伺服器基礎」。

系統服務

任何服務或應用程式都是一個潛在的被攻擊弱點，因此任何沒有必要的服務或執行檔都應停止使用或移除。在 MSBP 中，選擇性的服務以及任何沒有必要的服務都會停用。底下的這節詳細說明了在列印伺服器上必須被啓用的服務。

列印多工緩衝處理器

表 7.2：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
列印多工緩衝處理器	自動	自動	自動	自動

Print Spooler (列印多工緩衝處理器) 服務管理所有本機與網路的列印佇列，並控制所有的列印工作。Print Spooler 服務是 Windows 列印子系統的中心，並與印表機驅動程式及輸出/輸入 (I/O) 元件作溝通。

列印伺服器倚賴 Print Spooler 服務的正確運作。爲了讓列印伺服器爲用戶端處理列印工作，這服務必須設定成執行。透過以群組原則來保護與設定 Print Spooler 服務的起動模式，系統可將存取權僅授與伺服器管理員，來防止未授權或惡意的使用者設定或操作該服務。群組原則也可防止管理員不慎地停用該服務。基於這些原因，Print Spooler 設定值在本手冊所定義三個系統環境中，是設定成 Automatic (自動)。

其他安全性設定

透過 MSBP 套用的安全性設定，替列印伺服器提供了許多增強的安全性。然而，還有一些額外的事項需要考慮。這些步驟無法透過群組原則來完成，因此必須以手動方式去在所有的列印伺服器上執行。

保護知名帳戶

Microsoft Windows Server 2003 擁有許多無法刪除、但可重新命名的內建使用者帳戶。Windows 2003 內兩個最有名的內建帳戶為 Guest 與 Administrator。Guest 帳戶在預設狀態下將停用於成員伺服器和網域控制站上。

此設定不應該變更。內建的 Administrator 帳戶應該重新命名，而描述也應改變，以防止攻擊者使用知名的帳戶危害遠端的伺服器。

許多惡意程式碼的變型都在初次嘗試中使用內建的管理員帳戶來危害伺服器。近年來，此組態變更的價值已逐漸減少，因為現在嘗試侵入伺服器的攻擊工具會指定內建 Administrator 帳戶的安全性識別項 (SID) 來決定其真正的名稱。SID 指的是可唯一識別網路上每個使用者、群組、電腦帳戶和登入工作階段的數值。您不可能變更此內建帳戶的 SID。將本機管理員帳戶重新命名為唯一的名稱，可讓您的作業群組監視嘗試攻擊此帳戶的事件。

保護列印伺服器上的知名帳戶：

1. 在每個網域和伺服器上，重新命名 Administrator 和 Guest 帳戶，然後將其密碼變更為長而複雜的值。
2. 在伺服器上使用不同的名稱和密碼。若所有的網域和伺服器上都使用相同的帳戶名稱和密碼，可存取某台成員伺服器的攻擊者即可以相同的帳戶名稱和密碼來存取所有其他的伺服器。
3. 將帳戶描述變更為預設值以外的值，以防止他人輕易地識別出帳戶。
4. 將這些變更記錄在安全的位置。

注意：內建的 Administrator 帳戶可透過群組原則來重新命名。此設定值並未設定於本手冊所提供的任何安全性範本內，因為您應替您的環境選擇唯一的名稱。您可設定 Accounts：Rename administrator account 設定值，以便將此手冊所定義三個系統環境中的管理員帳戶全都重新命名。此設定值是群組原則中安全性選項 (Security Options) 設定的一部份。

保護服務帳戶

除非必要，否則千萬不要將服務設定成在網域帳戶的安全性內容底下執行。若伺服器已實體地受到危害，他人即可透過傾印 Local Security Authority (LSA) 秘密，輕鬆取得網域帳戶的密碼。

以 IPSec 篩選器封鎖連接埠

Internet Protocol Security (IPSec) 篩選器可提供有效的方法來增強伺服器所需的安全性等級。此手冊替手冊內所定義的高安全性環境建議此選擇性指引，以進一步地減少伺服器的攻擊面。

如需使用 IPSec 篩選器的詳細資訊，請參閱下列隨附手冊的第 11 章「Additional Member Server Hardening Procedures」：《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》。

下表列出了所有可建立於本手冊所定義高安全性環境之列印伺服器上的 IPSec 篩選器。

表 7.3：列印伺服器 IPSec 網路傳輸對應

服務	通訊協定	來源連接埠	目標連接埠	來源位址	目標位址	動作	鏡像
CIFS 伺服器	TCP	任意	445	任意	ME	允許	是
	UDP	任意	445	任意	ME	允許	是
NetBIOS 伺服器	TCP	任意	137	任意	ME	允許	是
	UDP	任意	137	任意	ME	允許	是
	UDP	任意	138	任意	ME	允許	是
	TCP	任意	139	任意	ME	允許	是
OnePoint 用戶端	任意	任意	任意	ME	MOM Server	允許	是
終端機服務	TCP	任意	3389	任意	ME	允許	是
網域成員	任意	任意	任意	ME	網域控制站	允許	是
網域成員	任意	任意	任意	ME	網域控制站 2	允許	是
所有傳入的傳輸資料	任意	任意	任意	任意	ME	封鎖	是

上表所列的所有規則都應在實作時加以鏡像。這可確保傳入伺服器內的任何網路傳輸資料亦可回到原本的伺服器中。

上表代表了應開啟哪些基底連接埠，以便讓伺服器執行其特定角色的功能。若伺服器擁有靜態的 IP 位址，這些連接埠就已足夠。若要提供額外的功能，可能還需要另外開啟其他的連接埠。例如，可能需要開啟 515 號連接埠才能夠掛接 LPR 印表機的列印伺服器。雖然開啟額外的連接埠可讓您環境中的列印伺服器更容易管理，不過，也可能會大大降低這些伺服器的安全性。

因為網域成員和網域控制站之間有大量的互動，特別是 RPC 和驗證傳輸，因此列印伺服器和所有的網域控制站之間，所有的通訊都允許傳輸。事實上，可以進一步限制它們之間的傳輸，但是大多數的環境都需要額外建立數十個篩選器，才能讓篩選器有效地保護伺服器。這可能會令 IPSec 原則的實作和管理變得極為困難。因為與列印伺服器互動的每個網域控制站都需建立類似的規則。若想要增加列印伺服器的可靠性和可用性，則需另外在您系統環境的所有網域控制站中增加規則。

如上所示地，若 Microsoft Operations Manager (MOM) 實作於環境中，所有的網路傳輸資料都必須可傳送於實作 IPSec 篩選器的伺服器和 MOM 伺服器之間。因為 MOM 伺服器和 OnePoint 用戶端 (向 MOM 主控台報告的用戶端應用程式) 之間有大量的互動，這是必要的。其他管理套件可能擁有類似的需求。若需要更大的安全性，您可設定 OnePoint 用戶端的篩選器動作，以便讓 IPSec 與 MOM 伺服器互相協商。此 IPSec 原則可透過隨機的高連接埠有效地封鎖傳輸，藉此禁止遠端程序呼叫 (RPC) 的傳輸。這將令伺服器的管理變得困難。因為這麼多的連接埠已經有效地關閉，終端機服務將被啟用。這可讓管理員執行遠端管理。

上述的網路傳輸對應將假設環境中包含了具備 Active Directory 能力的 DNS 伺服器。若使用獨立的 DNS 伺服器，可能還需要額外的規則。

實作 IPSec 原則應該不會嚴重地影響伺服器的效能。不過，您仍應在實作這些篩選器之前進行測試，以確保伺服器的必要功能和效能都可維持。您可能也會需要加入額外的規則來支援其他應用程式。

本手冊包含了一個 .cmd 檔，簡化了建立適用於列印伺服器的 IPSec 篩選器的工作。PacketFilters-Print.cmd 檔案使用 NETSH 命令來建立適當的篩選器。您必須修改這個 .cmd 檔，以包含您環境的網域控制站的 IP 位址。其指令碼包含了可加入兩個網域控制站的預留位置。若有需要，可將額外的網域控制站加至指令碼內。網域控制站的 IP 位址清單必須保持在最新狀態。

若 MOM 出現在環境之中，適當 MOM 伺服器的 IP 位址也必須指定於指令碼內。此指令碼並不會建立永續性篩選器。因此，伺服器需等到 IPSec Policy Agent 啟動時才會受到保護。如需建立永續性篩選器或建立更進階 IPSec 篩選器指令碼的詳細資訊，請參閱下列所附手冊的第 11 章「Additional Member Server Hardening Procedures」：《Threats and Countermeasures：Security Settings in Windows Server 2003 and Windows XP》。最後，此指令碼已設定成不指定它建立的 IPSec 原則。IP Security Policy Management 嵌入式管理單元可用來檢查建立的 IPSec 篩選器，並指定 IPSec 原則，以便讓它生效。

摘要

本章說明了伺服器的補強設定，以保護本手冊所定義三個用戶端環境中的列印伺服器之安全。大多數所討論的設定都是使用群組原則來設定與套用的。群組原則物件 (GPO) 是設計用來補足連結至網域控制站組織單位 (OU) 的「預設網域控制站原則」。「網域控制站基礎原則」(DCBP) 所包含的設定，將在任何給定的環境中，增強整個網域控制站的整體安全性。

某些討論的設定並不能使用群組原則來套用。針對這些狀況，本章提供了手動設定這些設定值的細節。此外，本章也提供建立與套用 IPSec 篩選器的細節，以控制可與列印伺服器進行通訊的網路傳輸類型。

詳細資訊

底下的資訊來源列出了在本產品發行之際，與執行 Windows Server 2003 的電腦所在環境中的列印伺服器密切相關的最新主題。

如需列印伺服器的概觀，請參閱“Technical Overview of Windows Server 2003 Print Services”，網址為：
<http://www.microsoft.com/windowsserver2003/techinfo/overview/print.mspx>。

如需列印伺服器詳細資訊，請參閱“What's New in File and Print Services”，網址為：
<http://www.microsoft.com/windowsserver2003/evaluation/overview/technologies/fileandprint.mspx>。

如需 IPSec 篩選器詳細資訊，請參閱“How To : Use IPSec IP Filter Lists in Windows 2000”，網址為：
<http://support.microsoft.com/default.aspx?scid=313190>。

8. 補強 IIS 伺服器

概觀

本章的重點在於補強您環境內 IIS 伺服器所需的指引和程序。爲了讓企業組織內部網路內的 Web 伺服器和應用程式能夠提供完善的安全性，每個 Microsoft® Internet Information Services (IIS) 伺服器，以及每個執行於這些伺服器上的網站和應用程式，都應防範可連至它們的用戶端電腦有任何不軌之舉。執行於每個 IIS 伺服器上的網站和應用程式也應防範執行於共同 intranet 內之其他 IIS 伺服器上的網站和應用程式。

爲了對惡意的使用者和攻擊者採取更主動出擊的態度，IIS 在預設狀態下並不會安裝在 Microsoft Windows® Server™ 2003 系統的成員之上。IIS 一開始將安裝在高度安全的“鎖定”模式之中。舉例來說，在預設狀態下，IIS 一開始只會提供靜態內容服務。諸如 Active Server Pages (ASP)、ASP.NET、Server Side Includes (SSI)、Web Distributed Authoring and Versioning (WebDAV) 發行和 Microsoft FrontPage® Server Extensions 等功能必須等到管理員啓用它們之後才有作用。這些功能和服務可透過 Internet Information Services Manger (IIS Manager) 中的 Web Service Extensions 節點來啓用。

IIS Manager 是專爲簡化 IIS 的管理而設計的圖形使用者介面 (GUI)。它包含了檔案和目錄管理的資源、應用程式集區的組態，以及安全性、效能和可靠性等功能。

本章的底下章節詳述了應實作的各式安全性補強設定，以增強在共同 intranet 中主控 HTML 內容之 IIS 伺服器的安全性。不過，爲了確保 IIS 伺服器安全無虞，您也應實作安全性監視、偵測和回應程序。

稽核原則設定

本手冊所定義三個系統環境中的 IIS 伺服器的稽核原則 (Audit Policy) 設定都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建立成員伺服器基礎」。MSBP 設定可確保所有相關的安全性稽核資訊都記錄於所有的 IIS 伺服器上。

使用者權限指定

本手冊所定義三個系統環境中的 IIS 伺服器的使用者權限設定 (User Rights Assignments) 都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建成立員伺服器基礎」。MSBP 和累加 IIS 群組原則之間的差異將描述於下列章節中。

拒絕從網路存取本電腦

表 8.1：設定值

網域控制站預設值	舊版用戶端	企業用戶端	高安全性
SUPPORT_388945a0	ANONYMOUS LOGON; 內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶	ANONYMOUS LOGON; 內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶	ANONYMOUS LOGON; 內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶

注意：ANONYMOUS LOGON、內建管理員、Support_388945a0、Guest 和所有非作業系統服務的帳戶都未包含於安全性範本內。對於您組織內的每個網域，這些帳戶和群組都有唯一的安全性識別碼 (SID)。因此，它們必須手動地加入。

Deny access to this computer from the network(拒絕從網路存取本電腦)此設定值可決定了哪些使用者無法存取網路上的電腦。此設定將會拒絕許多網路通訊協定，包括了以伺服器訊息區塊 (SMB) 為基礎的通訊協定、網路基本輸入/輸出系統 (NetBIOS)、Common Internet File System (CIFS)、Hypertext Transfer Protocol (HTTP) 和 Component Object Model Plus (COM+)。若此設定值和「Access this computer from the network」同時控制使用者帳戶，此設定值會蓋過「Access this computer from the network」設定值。替其他群組設定此使用者權限，可能會限制使用者在您的環境中執行委派管理工作的能力。

在第三章「建成立員伺服器基礎」中，此手冊建議將 Guests 群組包含於指定了此權限的使用者和群組清單內，以提供最高等級的安全性。不過，用來匿名存取 IIS 的 IUSR 帳戶在預設狀態下為 Guests 群組的成員。此手冊建議您從累加 IIS 群組原則中移除 Guests 群組，以確保您可在需要時，設定以匿名方式存取 IIS 伺服器。基於這些理由，本手冊所定義的三個系統環境都將 IIS 伺服器的「Deny access to this computer from the network(拒絕從網路存取本電腦)」設定值設成包含了 ANONYMOUS LOGON; 內建管理員; Support_388945a0; Guest; 所有非作業系統服務的帳戶。

安全性選項

本手冊所定義三個系統環境中的 IIS 伺服器的安全性選項 (Security Options) 設定都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建員成員伺服器基礎」。MSBP 設定可確保所有相關的安全性選項都一致地設定於所有的 IIS 伺服器上。

事件記錄檔設定

本手冊所定義三個系統環境中的 IIS 伺服器的事件記錄檔 (Event Log) 設定都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建員成員伺服器基礎」。MSBP 設定可確保企業內的所有 IIS 伺服器都一致地設定適當的事件記錄檔設定。

系統服務

爲了讓 IIS 將 Web 伺服器功能加至 Microsoft Windows Server™2003，下列三項服務必須啓用。累加 IIS 群組原則可確保這些服務都設成自動啓動。

注意：MSBP 會停用其他多個 IIS 的相關服務。FTP、SMTP 和 NNTP 即爲 MSBP 所停用的一些服務。若本手冊所定義三個系統環境中有任何一個需啓用上述任一個服務，就需要修改累加的 IIS 群組原則。

HTTP SSL

表 8.2：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
HTTPFilter	手動	自動	自動	自動

HTTP SSL 服務可讓 IIS 執行 Secure Sockets Layer (SSL) 功能。SSL 是建立安全通訊通道的開放性標準，可防止他人攔截重要資訊，例如信用卡號。其主要用途是在全球資訊網上啓用安全的電子金融交易，不過它也可運作於其他的 Internet 服務上。

若 HTTP SSL 服務已停止，IIS 將不會執行 SSL 功能。停用此服務將導致實際倚賴它的任何服務執行失敗。透過以群組原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器管理員，因此可防止未授權或惡意的使用者設定或操作該服務。群組原則也可防止管理員不慎地停用該服務。基於這些理由，本手冊所定義三個系統環境中的 IIS 伺服器都將 HTTP SSL 設定值設成 Automatic(自動)。

IIS Admin Service

表 8.3：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
IISADMIN	未安裝	自動	自動	自動

IIS Admin Service 可讓您管理 IIS 元件，例如 File Transfer Protocol (檔案傳輸通訊協定，簡寫爲 FTP)、應用程式集區、網站、Web 服務擴充功能和 Network News Transfer Protocol (網路新聞傳輸通訊協定，簡寫爲 NNTP) 與 Simple Mail Transfer Protocol (簡單郵件傳輸通訊協定，簡寫爲 SMTP) 虛擬伺服器。

IIS Admin Service 必須持續地執行，IIS 伺服器才能提供 Web、FTP、NNTP 和 SMTP 服務。若此服務停用，您就無法設定 IIS，也無法要求任何 Web 服務。透過以群組原則來保護與設定服務的起動模式，系統可將存取權只授與伺服器管理員，因此可防止未授權或惡意的使用者設定或操作該服務。群組原則也可防止管理員不慎地停用該服務。基於這些理由，本手冊所定義三個系統環境中的 IIS 伺服器都將 IIS Admin Service 設定值設成 Automatic(自動)。

World Wide Web Publishing Service

表 8.4：設定值

服務名稱	成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
W3SVC	未安裝	自動	自動	自動

World Wide Web Publishing Service 透過 IIS 嵌入式管理單元提供 Web 連接能力和網站管理。

World Wide Web Publishing Service 必須持續地執行，IIS 伺服器才能透過 IIS Manager 提供 Web 連接能力和管理。透過以群組原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器管理員，因此可防止未授權或惡意的使用者設定或操作該服務。群組原則也可防止管理員不慎地停用該服務。基於這些理由，本手冊所定義三個系統環境中的 IIS 伺服器都將 World Wide Web Publishing Service 設定值設成 Automatic(自動)。

其他安全性設定

安裝完 Windows Server 2003 和 IIS 之後，IIS 在預設狀態下只會傳輸靜態的 Web 內容。當網站和應用程式包含動態內容，或需要一個或多個額外的 IIS 元件時，每個額外的 IIS 功能都必須個別去啟用。不過，在此過程中，您務必確保您環境中每個 IIS 伺服器的攻擊弱點能夠盡量減少。若您組織中的網站包含了靜態內容，並且不需要任何其他的 IIS 元件，那麼預設的 IIS 組態就足以將您環境中 IIS 伺服器的被攻擊弱點降至最低。

透過 MSBP 套用的安全性設定替 IIS 伺服器提供了許多增強的安全性。但還有一些額外的事項需要考慮。這些步驟並無法透過群組原則來完成，而應手動地執行於所有的 IIS 伺服器上。

僅安裝必要的 IIS 元件

除了 World Wide Web Publishing Service 以外，IIS 6.0 還包含了其他元件和服務，例如 FTP 和 SMTP 等服務。IIS 元件和服務都是使用 Windows Components Wizard Application Server 來安裝與啟用，您可透過連按兩下「Control Panel」內的「Add or Remove Programs」來啟動此程式。安裝完 IIS 之後，網站和應用程式所需的所有必要 IIS 元件和服務都必須啟用。

- 若要安裝 Internet Information Services (IIS) 6.0 :
 1. 在 Control Panel 上連按兩下 Add or Remove Programs。
 2. 按一下 Add/Remove Windows Components 按鈕來啟動 Windows Components Wizard。
 3. 在 Components 清單中按一下 Application Server，接著再按 Details。
 4. 在 Application Server 對話方塊的 Subcomponents of Application Server 底下，按一下 Internet Information Services (IIS)，接著按 Details。
 5. 在 Internet Information Services (IIS) 對話方塊的 Subcomponents of Internet Information Services (IIS) 清單中執行下列工作：
 - 若要加入選擇性元件，請選取欲安裝元件旁邊的核取方塊。
 - 若要移除選擇性元件，請清除欲移除元件旁邊的核取方塊。
 6. 按一下 OK 直到您返回 Windows Component Wizard。
 7. 按一下 Next，接著按 Finish。

只有網站和應用程式所需的基本 IIS 元件和服務需要去啟用。啟用沒有必要的元件和服務只會增加 IIS 伺服器的被攻擊的弱點。

下列圖表顯示了 IIS 元件的位置和建議設定。

Application Server 對話方塊內的子元件如下所示：

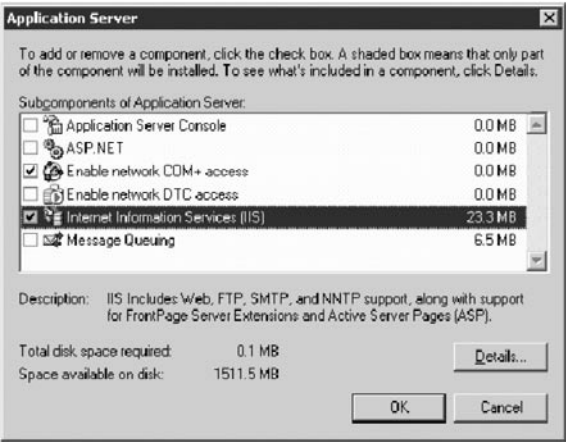


圖 8.1

Application Server 子元件 下表簡單地描述 Application Server 子元件，並建議何時該啓用它們。

表 8.5：Application Server 子元件

UI 中的元件名稱	設定值	設定邏輯
Application Server Console	停用	提供一個 Microsoft Management Console (MMC) 嵌入式管理單元，以管理所有的 Web Application Server 元件。在專用的 IIS 伺服器上並不需要此元件，因為它可使用 IIS Server Manager。
ASP.NET	停用	提供 ASP.NET 應用程式的支援。請在 IIS 伺服器執行 ASP.NET 應用程式時，啓用此元件。
Enable network COM+ access	啓用	允許 IIS 伺服器主控分散式應用程式的 COM+ 元件。此元件對於 FTP、BITS 伺服器擴充功能、World Wide Web Service 和 IIS Manager 等項目是必要的。
Enable network DTC access	停用	允許 IIS 伺服器主控會經由 Distributed Transaction Coordinator (DTC) 參與於網路交易中的應用程式。除非執行於 IIS 伺服器上的應用程式需要，否則請停用此元件。
Internet Information Services (IIS)	啓用	提供基本的 Web 和 FTP 服務。專用的 IIS 伺服器需要此元件。
Message Queuing	停用	注意：若此元件未啓用，那所有的子元件都會停用。

Internet Information Services (IIS) 對話方塊中的子元件如下所示：

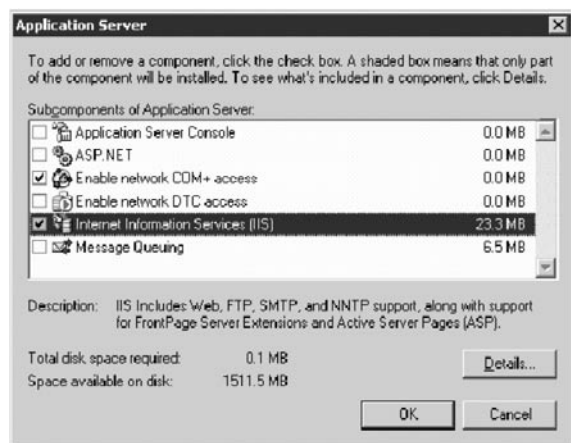


圖 8.2

IIS 子元件 下表簡單地描述 IIS 子元件，並建議何時該啟用它們。

表 8.6：IIS 子元件

UI 中的元件名稱	設定值	設定邏輯
Background Intelligent Transfer Service (BITS) server extension	啟用	BITS 是 Windows Update and Automatic(自動) Update 所使用的背景檔案傳輸機制。當您使用 Windows Update 或 Automatic(自動) Update 自動套用服務套件和 Hotfix 到 IIS 伺服器上時，就需要此元件。
Common Files	啟用	IIS 需要這些檔案，並且它們必須持續地啓用於 IIS 伺服器上。
File Transfer Protocol (FTP) Service	停用	允許 IIS 伺服器提供 FTP 服務。專用的 IIS 伺服器並不需要此服務。
FrontPage 2002 Server Extensions	停用	提供 FrontPage 的支援，以管理和發行網站。若沒有網站使用 FrontPage 擴充功能，此元件將停用於專用的 IIS 伺服器上。
Internet Information Services Manager	啟用	IIS 的管理介面。
Internet Printing	停用	提供 Web 型態的印表機管理，並讓印表機共用於 HTTP 上。專用的 IIS 伺服器並不需要此元件。

UI 中的元件名稱	設定值	設定邏輯
NNTP Service	停用	在 Internet 上散發、查詢、擷取和張貼 Usenet 新聞文章。專用的 IIS 伺服器並不需要此元件。
SMTP Service	停用	支援電子郵件的傳輸。專用的 IIS 伺服器並不需要此元件。
World Wide Web Service	啟用	提供 Web 服務、靜態和動態內容給用戶端。專用的 IIS 伺服器需要此元件。

Message Queuing 對話方塊內的子元件如下所示：

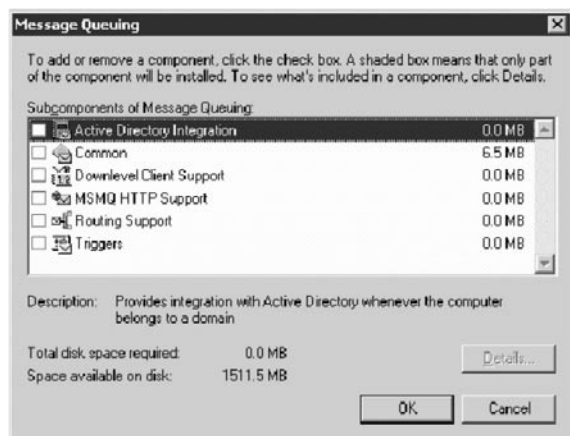


圖 8.3

Message Queuing 子元件

下表簡單地描述 Message Queuing 子元件，並建議何時該啓用它們。

表 8.7：Message Queuing 子元件

UI 中的元件名稱	設定值	設定邏輯
Active Directory Integration	停用	當 IIS 伺服器屬於某一網域時，即提供與 Microsoft Active Directory® 的整合。當執行於 IIS 伺服器上的網站和應用程式使用 Microsoft Message Queuing (MSMQ) 時就需要此元件。
Common	停用	IMSMQ 需要此元件。當執行於 IIS 伺服器上的網站和應用程式使用 MSMQ 時就需要此元件。
Downlevel Client Support	停用	讓您存取下游用戶端的 Active Directory 和網站辨識。當 IIS 伺服器的網站和應用程式使用 MSMQ 時就需要此元件。
MSMQ HTTP Support	停用	在 HTTP 傳輸上提供訊息的傳送與接收。當 IIS 伺服器的網站和應用程式使用 MSMQ 時就需要此元件。
Routing support	停用	替 MSMQ 提供存放及轉寄 (store-and-forward) 訊息以及有效率的路由服務當執行於 IIS 伺服器上的網站和應用程式使用 MSMQ 時就需要此元件。

Background Intelligent Transfer Service (BITS) Server Extensions 對話方塊內的子元件如下所示：



圖 8.4

Background Intelligent Transfer Service (BITS) Server Extensions 子元件 下表簡單地描述 Background Intelligent Transfer Service (BITS) Server Extensions 子元件，並建議何時該啟用它們。

表 8.8：Background Intelligent Transfer Service (BITS) Server Extensions 子元件

UI 中的元件名稱	設定值	設定邏輯
BITS management console snap-in	啟用	安裝 MMC 嵌入式管理單元來管理 BITS。當 Internet Server Application Programming Interface (ISAPI) 的 BITS 伺服器擴充功能啟用時，就需啟用此元件。
BITS server extension ISAPI	啟用	安裝 BITS ISAPI，以便讓 IIS 伺服器使用 BITS 來傳輸資料。當您使用 Windows Update 或 Automatic(自動) Update 自動套用服務套件和 Hotfix 到 IIS 伺服器上時，就需要此元件。若未使用 Windows Update 或 Automatic(自動) Update，則停用此元件。

World Wide Web Service 對話方塊內的子元件如下所示：

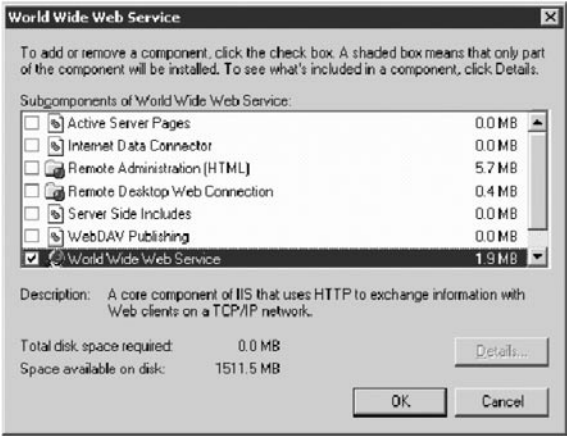


圖 8.5

World Wide Web Service 子元件 下表簡單地描述 World Wide Web Service 子元件，並建議何時該啓用它們。

表 8.9：World Wide Web Service 子元件

UI 中的元件名稱	設定值	設定邏輯
Active Server Pages	停用	提供 ASP 的支援。若 IIS 伺服器上沒有網站或應用程式使用 ASP，即停用此元件，或使用 Web 服務擴充功能來停用它。如需詳細資訊，請參閱本章的「僅啓用基本的 Web 服務擴充功能」小節。
Internet Data Connector	停用	透過副檔名為 .idc 的檔案提供動態內容的支援。若 IIS 伺服器上沒有網站或應用程式包含副檔名為 .idc 的檔案，即停用此元件，或使用 Web 服務擴充功能來停用它。如需詳細資訊，請參閱本章的「僅啓用基本的 Web 服務擴充功能」小節。

(接上頁)

Remote Administration (HTML)	停用	提供 HTML 介面來管理 IIS。改用 IIS Manager 來提供更輕鬆的管理，並減少 IIS 伺服器的被攻擊弱點。專用的 IIS 伺服器並不需要此功能。
Common	停用	包含 Microsoft ActiveX [®] 控制項和範例網頁，以主控終端機服務的用戶端連接。改用 IIS Manager 來提供更輕鬆的管理，並減少 IIS 伺服器的被攻擊弱點。專用的 IIS 伺服器並不需要此功能。
Server-Side Includes	停用	提供 .shtm、.shtml 和 .stm 檔的支援。若沒有執行於 IIS 伺服器上的網站或應用程式使用這些副檔名的 include 檔，即停用此元件。
WebDAV	停用	WebDAV 擴充了 HTTP/1.1 通訊協定，可讓用戶端發行、鎖定和管理 Web 上的資源。您可在專用的 IIS 伺服器上停用此元件，或使用 Web 服務擴充功能來停用它。如需詳細資訊，請參閱本章的「僅啓用基本的 Web 服務擴充功能」小節。
World Wide Web Service	啓用	提供 Web 服務、靜態和動態內容給用戶端。專用的 IIS 伺服器需要此元件。

僅啓用基本的 Web 服務擴充功能

許多執行在 IIS 伺服器上的網站和應用程式都將功能擴充到靜態網頁之外，還包括產生動態性內容。任何透過 IIS 伺服器所提供的功能去服務或擴充的動態內容都是使用 Web 服務擴充功能來完成的。

IIS 6.0 內的增強安全性功能可啓用或停用個別的 Web 服務擴充功能。在進行新的安裝之後，IIS 伺服器只會傳送靜態內容。動態內容功能可透過 IIS Manager 中的 Web Service Extensions 節點來啓用。這些擴充功能包括了 ASP.NET、SSI、WebDAV 和 FrontPage Server Extensions。

啓用所有的 Web 服務擴充功能可確保與現有的應用程式保有最高度的相容性；不過，這也會產生安全性的風險，因為當所有的擴充功能都啓用之後，由於啓用的功能未必是您環境的 IIS 伺服器所需，IIS 的被攻擊弱點將會增加。

爲了儘可能減少 IIS 伺服器的被攻擊弱點，在手冊所定義三個系統環境中的 IIS 伺服器上應只啓用必要的 Web 服務擴充功能。

只啓用執行於您環境之 IIS 伺服器上的網站和應用程式所必需的 Web 服務擴充功能，可增強安全性，因爲透過儘量減少伺服器功能，可減少每個 IIS 伺服器的被攻擊弱點。

下表列出了預定的 Web 服務擴充功能，並提供何時啓用每個擴充功能的細節。

表 8.10：啓用 Web 服務擴充功能

Web 服務擴充功能	啓用擴充功能的時機
Active Server Pages	執行於 IIS 伺服器上的一個或多個網站和應用程式包含了 ASP 內容。
ASP.NET v1.1.4322	執行於 IIS 伺服器上的一個或多個網站和應用程式包含了 ASP.NET 內容。
FrontPage Server Extensions 2002	執行於 IIS 伺服器上的一個或多個網站使用了 FrontPage 擴充功能。
Internet Data Connector (IDC)	執行於 IIS 伺服器上的一個或多個網站和應用程式使用了 IDC 來顯示資料庫資訊 (此內容包含了 .idc 和 .idx 檔)。
Server Side Includes (SSI)	執行於 IIS 伺服器上的一個或多個網站使用 SSI 指示詞來指示 IIS 伺服器將可重複使用的內容 (例如導覽列、網頁頁首或頁尾) 插入不同的網頁內。
Web Distributed Authoring and Versioning (WebDav)	IIS 上需要 WebDAV 支援，方能讓用戶端透明地發行與管理 Web 資源。

將內容放在專用的磁碟區中

IIS 將其預設網站的檔案儲存於 <systemroot>\inetpub\wwwroot 內，此處的 <systemroot> 爲安裝 Windows Server 2003 作業系統的磁碟機。

請將組成網站和應用程式的所有檔案和資料夾放在本手冊所定義三個系統環境的 IIS 伺服器上的專用磁碟區內。將這些檔案和資料夾放在 IIS 伺服器的專用磁碟區上 – 不包含作業系統 – 將有助於防止目錄往返式攻擊。目錄往返式攻擊指的是攻擊者要求取得位於 IIS 伺服器目錄結構外的檔案。

例如，cmd.exe 存在於 <systemroot>\System32 資料夾內。攻擊者可發出下列位置的要求：

..\..\Windows\system\cmd.exe，以嘗試叫用命令提示字元。

若網站內容是置於個別的磁碟區內，則這類目錄往返式攻擊就無法成功。其原因有二，首先，cmd.exe 上的存取權限已重設，這是 Windows Server 2003 基礎組建的一部份，爲的是將其存取範圍限制成更有用的使用者群組範圍內。其次，在進行完此變更之後，cmd.exe 所在的磁碟區和 Web 根目錄不同，而且目前並沒有已知的方法可使用這類攻擊來存取不同磁碟機上的命令。

除了安全性考量外，將網站和應用程式的檔案和資料夾放在專用的磁碟區上，可讓管理工作（例如備份和還原）更為容易。再者，將這類內容放在個別的專用實體磁碟機上，將有助於減少系統磁碟區上的磁碟競爭，並改善整體的磁碟存取效能。

設定 NTFS 權限

Windows Server 2003 會檢查 NTFS 檔案系統權限，以決定使用者或處理序對於特定檔案或資料夾進行的存取類型。

您應指定 NTFS 權限，以便允許或拒絕特定使用者存取本手冊所定義三個系統環境中的 IIS 伺服器上的網站。

NTFS 應與 Web 權限搭配使用，而非取代 Web 權限。NTFS 權限只會影響被允許或拒絕存取網站和應用程式內容的帳戶。網站權限則影響存取網站或應用程式的所有使用者。若某個目錄或檔案的 Web 權限和 NTFS 權限發生衝突，將會套用限制更大的設定。

若網站和應用程式不希望發生匿名存取，可以明確地拒絕匿名帳戶的存取。匿名存取發生於不具有已驗證憑證的使用者想要存取系統資源時。匿名帳戶包括了內建的 Guest 帳戶、Guests 群組和 IIS Anonymous 帳戶。此外，請刪除非 IIS 管理員之任何使用者的任何寫入存取權限。

下表建議您在 IIS 伺服器上所應套用的不同檔案類型的 NTFS 權限。不同的檔案類型可群組成個別的資料夾，藉此簡化套用 NTFS 權限的流程。

表 8.11：NTFS 權限

檔案類型	建議的 NTFS 權限
CGI 檔 (.exe、.dll、.cmd、.pl)	Everyone (execute) Administrators (full control) System (full control)
指令碼檔 (.asp)	Everyone (execute) Administrators (full control) System (full control)
Include 檔 (.inc、.shtm、.shtml)	Everyone (execute) Administrators (full control) System (full control)
靜態內容 (.txt、.gif、.jpg、.htm、.html)	Everyone (read-only) Administrators (full control) System (full control)

設定 IIS 網站權限

IIS 會檢查網站權限，可藉此決定能夠在網站內產生的動作類型，例如允許指令碼來源存取或目錄瀏覽。您應指定網站權限，以進一步地保護本手冊所定義三個系統環境中 IIS 伺服器上的網站。

網站權限可和 NTFS 權限搭配使用。您可針對特定的網站、目錄和檔案來設定它們。和 NTFS 權限不同的是，網站權限會影響每位想要存取 IIS 伺服器上網站的人。您可使用 IIS Manager 嵌入式管理單元來套用網站權限。

下表列出了 IIS 6.0 所支援的網站權限，並提供簡單的說明，解釋何時該指定任何給定的權限給網站。

表 8.12：IIS 6.0 網站權限

網站權限：	授與的權限：
Read (讀取)	使用者可檢視目錄或檔案的內容和屬性。此權限在預設狀態下是選取的。
Write (寫入)	使用者可變更目錄或檔案的內容和屬性。
Script Source Access (指令碼來源存取)	使用者可存取來源檔。若 Read 為啟用，那麼來源就可被讀取；若 Write 為啟用，那麼指令碼的原始程式碼就可變更。Script Source Access 包含了指令碼的原始程式碼。若 Read 和 Write 都未啟用，此選項將無法選用。重要：當 Script Source Access 啟用時，使用者即可檢視敏感資訊，例如使用者名稱和密碼。他們也可以變更執行於 IIS 伺服器上的原始程式碼，並且嚴重地影響伺服器的安全性和效能。
Directory browsing (目錄瀏覽)	使用者可檢視檔案清單和集合。
Log visits (記錄造訪)	替網站的每個造訪事件都建立一個記錄項目。
Index this resource (替此資源建立索引)	允許索引服務替資源建立索引。這可讓您在資源上進行搜尋。
Execute (執行)	下列選項決定了使用者的指令碼執行層級： • None – 不允許指令碼和執行檔執行於伺服器上。 • Scripts only – 只允許指令碼執行於伺服器上。 • Scripts and Executables – 同時允許指令碼和執行檔執行於伺服器上。

設定 IIS 記錄

本手冊建議您在本手冊所定義三個系統環境的 IIS 伺服器上啟用 IIS 記錄。

每個網站或應用程式都可建立個別的記錄檔。IIS 所記錄的資訊超越了 Microsoft Windows 所提供事件記錄或效能監視功能的範圍。IIS 記錄檔的資訊包括了誰造訪過網站、造訪者檢視什麼資料、資訊上一次檢視的時間。IIS 記錄檔可用來評估內容的普遍性、找出資訊瓶頸，或作為協助調查攻擊的資源。

IIS Manager 嵌入式管理單元可用來設定記錄檔格式、記錄檔排程和欲記錄的精確資訊。若要限制記錄檔的大小，請審慎地規劃要記錄哪些欄位。

當 IIS 記錄啓用時，IIS 會使用 W3C 擴充記錄檔格式 (W3C Extended Log File Format) 來建立每日的活動記錄檔，它們都儲存於您替 IIS Manager 內網站所指定的目錄內。

若要改善伺服器的效能，記錄檔應儲存於非系統的等量或等量/鏡像的磁碟區內。

再者，記錄檔也可將完整的 Universal Naming Convention (UNC) 路徑寫至網路上的遠端共用區。遠端記錄可讓管理員建立集中化的記錄檔案儲存與備份。不過，在網路上寫入記錄檔可能會降低伺服器的效能。

IIS 記錄可設成使用多個其他的 ASCII 或 Open Database Connectivity (ODBC) 記錄檔格式。ODBC 記錄可讓 IIS 將活動資訊儲存於 SQL 資料庫內。不過，請注意當 ODBC 記錄啓用時，IIS 將會停用核心模式的快取。基於此理由，實作 ODBC 記錄可能降低整體的伺服器效能。

控管上百個網站的 IIS 伺服器可啟用集中化的二進位記錄來改善記錄效能。集中化的二進位記錄可讓 IIS 伺服器上的所有網站將活動資訊寫至單一的記錄檔內。由於減少了需要個別儲存與分析的記錄檔個數，此作法可以大大改善 IIS 記錄流程的管理性和延展性。如需集中化二進位記錄的詳細資訊，請參閱 Microsoft TechNet 主題，"Centralized Binary Logging"，網址為：http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/log_binary.asp。

當 IIS 記錄檔在預設狀態下儲存於 IIS 伺服器時，只有伺服器管理員有權存取它們。若記錄檔的目錄或檔案擁有者未出現在 Local Administrators 群組內，HTTP.sys - IIS 6.0 內的核心模式驅動程式 - 會記錄一個錯誤到 NT 事件記錄檔內。此錯誤指出了目錄或檔案的擁有者並未出現在 Local Administrators 群組內，該記錄將會暫時存放在網站內，直到擁有者被加至 Local Administrators 群組內，或現有的目錄或記錄檔已刪除。

以手動方式將唯一的安全性群組加至使用者權限設定內

大多數經由 MSBP 套用的使用者權限設定 (User Rights Assignments) 都有適當的安全性群組指定於本手冊所附的安全性範本內。不過，仍有一些帳戶和安全性群組無法包含於範本之中，因為其安全性識別項 (SID) 僅適用於個別的 Windows 2003 網域。可以手動設定的使用者權限設定列出如下。

警告：下表包含了內建 Administrator 帳戶的值。請小心，勿將 Administrator 帳戶和內建的 Administrator 安全性群組搞混了。若 Administrators 安全性群組已加至底下的任一個拒絕存取使用者權限中，您需要登入於本機來訂正此錯誤。此外，內建管理員帳戶可能已根據第三章「建立成員伺服器基礎」所述的一些建議重新命名。在加入 Administrator 帳戶時，請記得指定重新命名的帳戶。

表 8.13：手動加入使用者權限設定

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
拒絕從網路存取此電腦	內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶	內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶	內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶

警告：所有非作業系統服務的帳戶包括了企業內特定應用程式所使用的服務帳戶。這並未包含 LOCAL SYSTEM、LOCAL SERVICE 或 NETWORK SERVICE 帳戶，它們都是作業系統使用的內建帳戶。

保護知名帳戶

Windows Server 2003 擁有許多無法刪除、但可重新命名的內建使用者帳戶。Windows 2003 內兩個最有名的內建帳戶為 Guest 與 Administrator。

Guest 帳戶在預設狀態下將停用於成員伺服器和網域控制站上。此設定不應該變更。內建的 Administrator 帳戶應該重新命名，而描述也應改變，以防止攻擊者使用知名的帳戶危害遠端的伺服器。

許多惡意程式碼的變型都在初次嘗試中使用內建的管理員帳戶來危害伺服器。近年來，此組態變更的價值已逐漸減少，因為現在嘗試侵入伺服器的攻擊工具會指定內建 Administrator 帳戶的安全性識別項 (SID) 來決定其真正的名稱。SID 指的是可唯一識別網路上每個使用者、群組、電腦帳戶和登入工作階段的數值。您不可能變更此內建帳戶的 SID。將本機管理員帳戶重新命名為唯一的名稱，可讓您的作業群組監視嘗試攻擊此帳戶的事件。

• 要保護 IIS 伺服器上的知名帳戶：

1. 在每個網域和伺服器上，重新命名 Administrator 和 Guest 帳戶，然後將其密碼變更為長而複雜的值。
2. 在伺服器上使用不同的名稱和密碼。若所有的網域和伺服器上都使用相同的帳戶名稱和密碼，那麼可存取某台成員伺服器的攻擊者即可以相同的帳戶名稱和密碼來存取所有其他的伺服器。
3. 將帳戶描述變更為預設值以外的值，以防止他人輕易地識別出帳戶。
4. 將這些變更記錄在安全的位置。

注意：內建的 Administrator 帳戶可透過群組原則來重新命名。此設定值並未設定於本手冊所提供的任何安全性範本內，因為您應替您的環境選擇唯一的名稱。您可設定 Accounts:Rename administrator account 設定值，以便將此手冊所定義三個系統環境中的管理員帳戶全都重新命名。在群組原則中，此設定值是安全性選項設定值的一部份。

保護服務帳戶

除非絕對必要，否則千萬不要將服務設定成執行於網域帳戶的安全性內容底下。若伺服器已實體地受到危害，他人即可透過傾印 Local Security Authority (LSA) 秘密，輕鬆取得網域帳戶的密碼。

以 IPSec 篩選器封鎖連接埠

Internet Protocol Security (IPSec) 篩選器可提供有效的方法來增強伺服器所需的安全性等級。此手冊替手冊內所定義的高安全性環境建議此選擇性指引，以進一步地減少伺服器的被攻擊弱點。

如需使用 IPSec 篩選器的詳細資訊，請參閱下列隨附手冊的第 11 章「Additional Member Server Hardening Procedures」：《Threats and Countermeasures:Security Settings in Windows Server 2003 and Windows XP》。

下表列出了所有可建立於本手冊所定義高安全性環境之 DHCP 伺服器上的 IPSec 篩選器。

表 8.14：DHCP 伺服器 IPSec 網路傳輸對應

服務	通訊協定	來源	目標連接埠	來源連接埠	目標位址	位址動作	鏡像
OnePoint 用戶端	任意	任意	任意	ME	MOM Server	允許	是
終端機服務	TCP	任意	3389	任意	ME	允許	是
網域成員	任意	任意	任意	ME	網域控制站	允許	是
網域成員	任意	任意	任意	ME	網域控制站 2	允許	是
HTTP Server TCP	任意	80	任意	ME	允許	是	
HTTPS Server TCP	任意	443	任意	ME	允許	是	
所有傳入的傳輸資料	任意	任意	任意	任意	ME	封鎖	是

上表所列的所有規則都應在實作時加以鏡像。這可確保傳入伺服器內的任何網路傳輸資料亦可回到原本的伺服器中。

上表代表了應開啓哪些基底連接埠，以便讓伺服器執行其角色的相關功能。若伺服器擁有靜態的 IP 位址，這些連接埠就已足夠。若要提供額外的功能，可能還需要開啓額外的連接埠。開啓額外的連接埠可讓您環境中的 IIS 伺服器更容易管理，不過，它們可能會大大降低這些伺服器的安全性。

因為網域成員和網域控制站之間有大量的互動，特別是 RPC 和驗證傳輸，所有的通訊都允許傳輸於 IIS 伺服器和所有的網域控制站之間。它們之間的傳輸可以進一步地限制，但是大多數的環境都需要建立數十個額外的篩選器，才能讓篩選器有效地保護伺服器。這可能會令 IPSec 原則的實作和管理變得極為困難。會與 IIS 伺服器互動的每個網域控制站都需建立類似的規則。要增加 IIS 伺服器的可靠性和可用性，通常都需替環境中的所有網域控制站增加規則。

如上所示地，若 Microsoft Operations Manager (MOM) 實作於環境中，所有的網路傳輸資料都必須可傳送於實作 IPSec 篩選器的伺服器和 MOM 伺服器之間。因為 MOM 伺服器和 OnePoint 用戶端 (向 MOM 主控台報告的用戶端應用程式) 之間有大量的互動，這是必要的。其他管理套件可能擁有類似的需求。若需要更大的安全性，您可設定 OnePoint 用戶端的篩選器動作，以便與 MOM 伺服器協商 IPSec 的相關議題。

此 IPSec 原則可透過隨機的高連接埠有效地封鎖傳輸，藉此禁止遠端程序呼叫 (RPC) 的傳輸。這將令伺服器的管理變得困難。因為這麼多的連接埠已經有效地關閉，終端機服務將被啓用。這可讓管理員執行遠端管理。

上述的網路傳輸對應將假設環境中包含了具備 Active Directory 能力的 DNS 伺服器。若使用獨立的 DNS 伺服器，可能還需要額外的規則。

實作 IPSec 原則應該不會嚴重地影響伺服器的效能。不過，您仍應在實作這些篩選器之前進行測試，以確保伺服器的必要功能和效能都可維持。您可能也需要加入額外的規則來支援其他應用程式。

本手冊包含了一個 .cmd 檔，可讓您更輕鬆地建立適用 IIS 伺服器的 IPSec 篩選器。PacketFilters-IIS.cmd 檔使用 NETSH 命令來建立適當的篩選器。您必須修改此 .cmd 檔，以包含您環境之網域控制站的 IP 位址。指令碼包含了預留位置來加入兩個網域控制站。若有需要，可再加入額外的網域控制站。網域控制站的 IP 位址清單必須保持在最新狀態。若 MOM 出現在環境之中，適當 MOM 伺服器的 IP 位址也必須指定於指令碼內。此指令碼並不會建立永續性篩選器。

因此，伺服器需等到 IPSec Policy Agent 啟動時才會受到保護。如需建立永續性篩選器或建立更進階 IPSec 篩選器指令碼的詳細資訊，請參閱下列所附手冊的第 11 章「Additional Member Server Hardening Procedures」：《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》。最後，此指令碼已設定成不指定它建立的 IPSec 原則。IP Security Policy Management 嵌入式管理單元可用來檢查建立的 IPSec 篩選器，並指定 IPSec 原則，以便讓它生效。

摘要

本章說明了伺服器的補強設定，以保護本手冊所定義三個系統環境中的 IIS 伺服器。大多數所討論的設定都是使用群組原則來設定與套用的。群組原則物件 (GPO) 是設計用來補足連結至網域控制站組織單位 (OU) 的「預設網域控制站原則」。「網域控制站基礎原則」(DCBP) 所包含的設定，將在任何給定的環境中，增強整個網域控制站的整體安全性。

某些討論的設定並不能使用群組原則來套用。針對這些狀況，本章提供了手動設定這些設定值的細節。此外，本章也提供建立與套用 IPsec 篩選器的細節，以控制可與 IIS 伺服器進行通訊的網路傳輸類型。

詳細資訊

底下的資訊來源列出了在本產品發行之際，與執行 Windows Server 2003 的電腦所在環境中的 IIS 伺服器密切相關的最新主題。

如需在 IIS 5.0 中啟用記錄的相關資訊，請參閱“HOW TO:Enable Logging in IIS 5.0”，網址為：
<http://support.microsoft.com/default.aspx?scid=313437>。

如需此主題的相關資訊，請參閱“Enable Logging”，網址為：
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/log_enablelogging.asp。

如需記錄網站活動的相關資訊，請參閱“Logging Site Activity”，網址為：
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/log_aboutlogging.asp。

如需擴充記錄的相關資訊，請參閱“Customizing W3C Extended Logging”，網址為：
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/log_customw3c.asp。

如需集中化二進位記錄的相關資訊，請參閱“Centralized Binary Logging”，網址為：
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/log_binary.asp。

如需遠端記錄的相關資訊，請參閱“Remote Logging”，網址為：
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/log_remote.asp。

如需產生、檢視或瞭解安全性記錄檔 (稽核) 的相關資訊，請造訪 Microsoft TechNet 的安全性網站，網址為：
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/server/sec_security.asp。

如需 IIS 6.0 的額外資訊，請造訪 TechNet 網站：
<http://www.microsoft.com/technet/prodtechnol/windowsnetserver/proddocs/server/iiswelcome.asp>。

如需 IPsec 篩選的詳細資訊，請參閱“How To:Use IPsec IP Filter Lists in Windows 2000”，網址為：
<http://support.microsoft.com/default.aspx?scid=313190>。

9. 補強 IAS 伺服器

概觀

本章提供補強建議及相關資源以保護執行 Microsoft® Windows Server 2003 的 Internet Authentication Service (網際網路驗證服務，簡稱為 IAS) 伺服器之安全。IAS 是一個 Remote Authentication Dial-in User Service (遠端驗證撥號使用者服務，簡稱為 RADIUS) 伺服器，它使得使用者的驗證、授權和帳戶能夠集中管理。IAS 可以用來驗證在 Windows Server 2003、Windows NT 4.0 或 Windows 2000 網域控制站上資料庫的使用者。此外，IAS 支援多種網路存取伺服器 (NAS)，包括 Routing and Remote Access (路由及遠端存取，簡稱為 RRAS)。

RADIUS 隱藏機制使用了 RADIUS 共用秘密、需求驗證器 (Request Authenticator) 和 MD5 雜湊演算法，來加密使用者密碼和其他屬性，例如通道密碼和 MS-CHAP-MPPE-Keys。RFC 2865 特別提到一個潛在的需求，就是評估威脅環境、並決定是否應使用額外的安全防護。

您可以藉由使用 Internet Protocol Security (網際網路通訊協定安全性，簡稱為 IPSec) 與 Encapsulating Security Payload (隱藏安全性負載量，簡稱為 ESP)，以及一個加密演算法，如 Triple DES (3DES) 來提供隱藏的屬性附加的保護，並為整個 RADIUS 訊息提供資料機密性。

Windows Server 2003 出廠時的預設值即已設成安全的狀態。為增進本章的可用性，此處只包含了那些由 MSBP 所作修改的設定。如需 MSBP 設定的詳細資訊，請參閱第三章「建成立員伺服器基礎」。如需所有預設值的相關資訊，請參閱所附的手冊，《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》。

注意：為 IAS 伺服器角色所開的設定值處方只針對企業用戶端環境做測試。因此，像 IPSec 篩選器和 DoS 攻擊資訊這些對本手冊其他大多數伺服器角色特定的陳述，就未包括在此處。

稽核原則

本手冊所定義三個環境中的 IAS 伺服器的稽核原則 (Audit Policy) 設定都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建立成員伺服器基礎」。MSBP 設定可確保所有相關的安全性稽核資訊都記錄於所有的 IAS 伺服器上。

使用者權限設定

本手冊所定義三個環境中的 IAS 伺服器的使用者權限設定 (User Rights Assignments) 也都是透過 MSBP 去設定。如需 MSBP 的詳細資訊，請參閱第三章「建立成員伺服器基礎」。MSBP 的設定可確保對 IAS 伺服器適當的存取是一致地設定於整個企業中。

安全性選項

本手冊所定義三個環境中的 IAS 伺服器的安全性選項 (Security Options) 設定也都是由 MSBP 來設定。如需 MSBP 的詳細資訊，請參閱第三章「建立成員伺服器基礎」。MSBP 的設定可確保對 IAS 服務伺服器適當的存取是一致地設定於整個企業中。

事件記錄檔

本手冊所定義三個環境中的 IAS 伺服器的事件記錄檔 (Event Log) 設定也都是由 MSBP 來設定。如需 MSBP 的詳細資訊，請參閱第三章「建立成員伺服器基礎」。

系統服務

任何服務或應用程式都是一個潛在的被攻擊弱點，因此任何沒有必要的服務或執行檔都應停止使用或移除。在 MSBP 中，選擇性的服務以及任何沒有必要的服務都會停用。

基於此理由，本手冊對於 IAS 伺服器角色的建議未必適用於您的環境。請依需要調整 IAS 伺服器群組原則的建議，以符合您組織的需求。

IAS 服務

表 9.1：設定

服務名稱	成員伺服器預設值	企業用戶端
IAS	未安裝	自動

IAS Service 設定為 RADIUS 通訊協定實作 IETF 標準，以致能使用異質性網路存取設備。如果停用這設定，會導致驗證需求的失敗轉移到可用的備份 IAS 伺服器去。假使沒有可用的備份 IAS 伺服器，使用者就不能連接到網路。停用這服務也會造成任何依賴它執行的服務執行失敗。

IAS Service 設定對 IAS 伺服器角色是必需的。為了讓 IAS 伺服器能夠對用戶端的驗證需求做出回應，此服務必須被執行。使用群組原則來保護與設定這服務的起動模式，系統可將存取權只授與伺服器管理員，因此可防止未授權或惡意的使用者設定或操作該服務。群組原則也可防止系統管理員不慎停用該服務。

其他安全性設定

透過 MSBP 套用的安全性設定替 IAS 伺服器提供了許多增強的安全性。然而，還有一些額外的事項需要考慮。這些步驟並不能透過群組原則來執行，應該手動地在所有的 IAS 伺服器上來完成。

保護知名帳戶

Windows Server 2003 擁有許多無法刪除、但可重新命名的內建使用者帳戶。Windows 2003 內兩個最有名的內建帳戶為 Guest 與 Administrator。

Guest 帳戶在預設狀態下在成員伺服器和網域控制站上是設成停用的。而此設定也不應該變更。內建的 Administrator 帳戶應該重新命名，而描述也應改變，以防止攻擊者使用知名的帳戶危害遠端的伺服器。

許多惡意程式碼的變型在初次嘗試中使用內建的 Administrator 帳戶來企圖危害伺服器。近年來，此組態變更的價值已逐漸減少，因為現在嘗試侵入伺服器的攻擊工具會指定內建 Administrator 帳戶的安全性識別項 (SID) 來決定其真正的名稱。SID 指的是可唯一識別網路上每個使用者、群組、電腦帳戶和登入工作階段的數值。您不可能變更此內建帳戶的 SID。將本機管理員帳戶重新命名為唯一的名稱，可讓您的作業群組監視嘗試攻擊此帳戶的事件。

• 保護 IAS 伺服器上的知名帳戶：

1. 在每個網域和伺服器上，重新命名 Administrator 和 Guest 帳戶，然後將其密碼變更為長而複雜的值。
2. 在伺服器上使用不同的名稱和密碼。若所有的網域和伺服器上都使用相同的帳戶名稱和密碼，可存取某台成員伺服器的攻擊者即可以相同的帳戶名稱和密碼來存取所有其他的伺服器。
3. 將帳戶描述變更為預設值以外的值，以防止他人輕易地識別出帳戶。
4. 將這些變更記錄在安全的位置。

注意：內建的 Administrator 帳戶可透過群組原則來重新命名。此設定值並未設定於本手冊所提供的任何安全性範本內，因為您應替您的環境選擇唯一的名稱。您可設定 Accounts：Rename administrator account 設定值，以便將此手冊所定義三個環境中的管理員帳戶全都重新命名。此設定值是群組原則的安全性選項 (Security Options) 設定的一部份。

保護服務帳戶

除非絕對必要，否則千萬不要將服務設定成在網域帳戶的安全性內容底下執行。若伺服器已實體地受到危害，他人即可透過傾印 Local Security Authority (LSA) 秘密，輕鬆取得網域帳戶的密碼。

摘要

本章說明了為保護本手冊所定義企業用戶端環境的 IAS 伺服器安全，而必需對伺服器所做的補強設定。這些設定可能也適用於本手冊所定義的其他環境，但他們並未經過測試與確認無誤。這邊所討論的設定都是依群組原則來設定與套用。群組原則物件 (GPO) 是設計用來補足連結至網域控制站組織單位 (OU) 的「預設網域控制站原則」。「網域控制站基礎原則」(DCBP) 所包含的設定，將在任何給定的環境中，增強整個網域控制站的整體安全性。

詳細資訊

底下的資訊來源列出了在本產品發行之際，本手冊中詳細談到的 Windows Server 2003 和 IAS 伺服器角色密切相關的最新主題。

如需 IAS 的詳細資訊，請參閱“Understanding IAS on Windows Server 2003”，網址為
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_ias_understanding.asp。

如需 IAS 與安全性的詳細資訊，請參閱 TechNet 的文章“Security information for IAS”，網址為
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_ias_security_issues.asp。

如需 Windows Server 2003 上的 IAS 與防火牆的資訊，請參閱“IAS and firewalls”，網址為
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/server/sag_ias_firewall.asp。

如需 RADIUS 的資訊，請參閱“Remote Authentication Dial In User Service (RADIUS)”，網址為
<http://www.cis.ohio-state.edu/cgi-bin/rfc/rfc2865.html>。

10. 補強憑證服務伺服器

概觀

本章將提供您完整的指引，以保護您系統環境中 Microsoft® 憑證服務 (Certificate Services) 伺服器的作業系統。雖然本章包含您需要完成這工作的所有資訊，但是指引內容並未詳細告訴您如何在您系統環境中，建立一個安全的憑證服務基礎架構，或是部署一個憑證授權單位。這些主題在以下這些文件中有深入探討：Microsoft Windows Server 2003 產品文件中的 Windows Server 2003 Resource Kit 以及 Microsoft Web 網站上有關這主題的白皮書。其他資訊可在所附的這份手冊找到：Securing Wireless LANs - a Windows Server 2003 Certificate Services Solution，其網址為 <http://go.microsoft.com/fwlink/?LinkId=14843>。

Windows Server 2003 出廠時的預設值即已設成安全的狀態。為增進本章的可用性，本章只說明那些由 MSBP 所作修改的設定。如需 MSBP 內設定的相關資訊，請參閱第三章「建成立員伺服器基礎」。如需所有預設值的相關資訊，請參閱所附的手冊，《Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP》。

您必須要在您系統環境中的某些憑證服務伺服器上，安裝 Microsoft 網際網路資訊服務 (Internet Information Services，簡稱為 IIS)，好使他們能分發憑證授權單位 (Certificate Authority，簡稱為 CA) 的憑證和憑證廢止清單 (Certificate Revocation Lists，簡稱為 CRL)。IIS 也用來掛接憑證服務伺服器的 Web 會員登入的網頁，允許非 Microsoft Windows? 的用戶端可以登入會員憑證。在第八章「補強 IIS 伺服器」中所述，如何安全地安裝 IIS 的程序，是使用本章資訊前事先需瞭解的。

此外，如果您在您的 CA 上安裝 IIS，那麼您必須先套用第八章的安全性設定範例到您的憑證服務伺服器，再根據本章為伺服器角色詳細列出的設定值去做設定。

注意：在簡化的環境中，發行 CA 伺服器可用來掛接於 Web 伺服器、CA 憑證以及 CRL 下載點。然而，請考慮在您系統環境中使用一個獨立的 Web 伺服器以增進您的 CA 的安全性。

IIS 是讓非 Windows 的用戶端用來裝載憑證伺服器登入會員網頁，以及分發 CA 憑證和 CRL 下載點。Microsoft 建議您不要把 IIS 安裝在憑證授權單位 (CA) 伺服器的根節點。如果可能的話，您也應該避免在您系統環境中負責發行和任何仲裁的 CA 上執行 IIS。比較安全的作法，是把 CA 憑證和 CRL 的 Web 下載點掛接在另一台伺服器，而非 CA 伺服器本身。也許會有許多憑證使用者（不論內部或外部的）需要讀取 CRL 或 CA 鍊的資訊，但是並沒有必要允許他們可存取 CA。如果下載點是掛接在 CA 本身，這個限制就不可能達到了。

注意：為憑證伺服器角色所開的設定值處方，只能在企業用戶端環境作測試。因此，IPSec 篩選器和拒絕服務 (DoS) 這些關於本手冊其他伺服器角色特定的資訊，本章就不做討論。

稽核原則設定

本手冊所定義企業用戶端環境的憑證服務伺服器的稽核原則 (Audit Policy) 設定都是由 MSBP 來設定。如需 MSBP 的詳細資訊，請參閱第三章「建立成員伺服器基礎」。MSBP 設定可確保所有相關的安全性稽核資訊都記錄於所有的憑證服務伺服器上。

使用者權限設定

本手冊所定義企業用戶端環境中、憑證服務伺服器之使用者權限設定 (User Rights Assignments)，都是由 MSBP 來設定。如需 MSBP 的詳細資訊，請參閱第三章「建立成員伺服器基礎」。MSBP 的設定可確保對憑證服務伺服器適當的存取是一致地設定於整個企業中。

安全性選項

群組原則的安全性選項，是用來啓用或停用電腦的安全性設定，例如，資料的數位簽章、Administrator 和 Guest 帳戶名稱、軟式磁碟機和 CD-ROM 磁碟機的存取、驅動程式安裝行為以及登入提示。

在 Windows Server 2003 中，安全性選項設定可以在「群組原則物件編輯器」(Group Policy Object Editor) 的以下這位置來設定：

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

本節中以下各表，包括了對本手冊所定義企業用戶端環境的憑證服務伺服器角色的安全性選項設定。

裝置：限制 CD-ROM 只能由本機登入的使用者存取

表 10.1：設定值

成員伺服器預設值	企業用戶端
停用	啓用

Devices：Restrict CD-ROM access to locally logged-on user only (裝置：限制CD-ROM 只能由本機登入的使用者存取) 此設定值可決定本機和遠端的使用者是否可同時存取 CD-ROM。啓用這設定只允許互動式登入的使用者來讀取可移除的 CD-ROM 媒體。不過，如果這設定被啓用，但沒有人以互動方式登入，使用者則可以透過網路存取 CD-ROM。

在有人登入伺服器本機控制台時，透過網路連接到憑證服務伺服器的使用者就不能使用伺服器的 CD-ROM。若是服務網路使用者的 CD 自動點唱機系統，則不建議啓用此設定。不過，啓用此設定可以防止駭客從這些伺服器上的 CD-ROM 執行具破壞性的程式。在 CA 上，系統管理者可能會將敏感重要的資料由 CD-ROM 複製到伺服器，或由伺服器複製出來；這設定可防止除了本機登入的管理者以外的任何人存取資料。因此，在本手冊所定義之企業用戶端系統環境中是設成啓用的。

裝置：限制 CD-ROM 只能由本機登入的使用者存取

表 10.2：設定值

成員伺服器預設值	企業用戶端
停用	啟用

Devices：Restrict floppy access to locally logged-on user only(裝置：限制 CD-ROM 只能由本機登入的使用者存取) 此設定值可決定本機和遠端的使用者是否可同時存取磁片媒體。啟用這設定只允許互動式登入的使用者來存取可移除的磁片媒體。不過，如果這設定被啟用，但沒有人以互動式登入，使用者便可以透過網路來存取磁片。

透過網路連接到憑證服務伺服器的使用者，在有人登入伺服器本機控制台時，就不能使用任何安裝在伺服器的軟式磁碟機。總之，啟用此設定可以防止駭客從這些伺服器上的軟式磁碟機執行具破壞性的程式。在CA上，系統管理者可能會將敏感重要的資料由 CD-ROM 複製到伺服器，或由伺服器複製出來；這設定可防止除了本機登入的管理者以外的任何人存取資料。因此，在本手冊所定義之企業用戶端系統環境中是設成啟用的。

系統密碼：使用 FIPS 相容演算法於加密、雜湊和簽章

表 10.3：設定值

成員伺服器預設值	企業用戶端
停用	啟用

System cryptography：Use FIPS compliant algorithms for encryption, hashing, and signing (系統密碼：使用 FIPS 相容演算法於加密、雜湊和簽章) 此設定決定「傳輸層安全性/安全封包層」(Transport Layer Security/Secure Sockets Layer，簡稱為 TLS/SSL) 的安全性提供者 (Security Provider) 是否只支援 TLS_RSA_WITH_3DES_EDE_CBC_SHA 密碼套件。事實上，這意味著 (若可行的話) 提供者只支援 TLS 通訊協定作為一個用戶端和一個伺服器。

TLS/SSL 安全性提供者使用：

- 三重資料加密標準 (Data Encryption Standard，簡稱為 DES) 加密演算法於 TLS 傳輸加密。
- Rivest、Shamir 和 Adelman (RSA) 公開金鑰演算法於 TLS 金鑰交換和驗證(RSA 是由 RSA Data Security, Inc. 所發展的一個公開金鑰加密技術)。
- SHA-1 雜湊演算法於 TLS 的雜湊需求。

對加密檔案系統服務 (Encrypting File System Service，簡稱為 EFS)，TLS/SSL 安全性提供者只支援三重 DES 加密演算法來加密 Windows NTFS 檔案系統提供的檔案資料。預設狀態下，EFS 是使用 DES 演算法來加密檔案資料。

啓用此設定能確保您系統環境中履行伺服器角色的電腦，將可使用可用、最強大的演算法來作數位加密、雜湊和簽章。這能使未經授權的使用者破壞數位加密或簽章資料的風險降到最低。基於這些理由，對本手冊中所定義的企業用戶端系統環境，是將這設定值設成啓用。

注意：若用戶端已啓用此設定，則無法透過數位加密或簽章的通訊協定來與不支援這些演算法的伺服器進行傳輸。不支援這些演算法的網路用戶端，則無法使用需要作為網路傳輸的伺服器。例如，很多以 Apache 為基礎的 Web 伺服器都設定成不支援 TLS。如果您啓用這設定，您也必須把 Internet Explorer 設定成使用 TLS，其步驟如下：開啓 Internet Explorer 的 Tools (工具) 功能表的 Internet Options (網際網路選項) 對話方塊，並點選該對話方塊的 Advanced (進階) 標籤，然後把 Settings (設定) 清單往下捲，並點選 Use TLS 1.0 (使用 TLS 1.0) 核取方塊。您也可以透過群組原則或用「Internet Explorer Administrators Kit」來設定此設定值。

事件記錄檔設定

本手冊所定義企業用戶端系統環境的憑證服務伺服器的事件記錄檔 (Event Log) 設定都是由 MSBP 來設定。如需 MSBP 的詳細資訊，請參閱第三章「建立成員伺服器基礎」。

系統服務

任何服務或應用程式都是一個潛在的被攻擊弱點，因此任何沒有必要的服務或執行檔都應停止使用或移除。在 MSBP 中，選擇性的服務以及任何沒有必要的服務都會停用。在 MSBP 中，這些選擇性的服務，以及所有其他非必要的服務都會停用。

在執行 Windows Server 2003 作為憑證服務伺服器的電腦上，還是有其他非必要的服務設成啟用狀態。這些服務的用途和安全性經常成為爭議的焦點。基於此理由，本章中對於這伺服器角色的建議未必適用於您的環境。請依需要調整憑證伺服器群組原則的建議，以符合您組織的需求。

系統服務設定可在 Windows Server 2003 的「群組原則物件編輯器」中的以下位置作設定：

Computer Configuration\Windows Settings\Security Settings\System Services\

以下的表包括了本手冊所定義企業用戶端系統環境的憑證服務伺服器角色漸進的原則服務設定。

憑證服務

表 10.4：設定值

服務名稱	成員伺服器預設值	企業用戶端
CertSvc	未定義	自動

Certificate Services 是 Windows Server 2003 核心作業系統的一部份，使得企業可自己擔任 CA。此服務是憑證服務伺服器運作正常所必須的。這些服務用來發行和管理應用程式的數位憑證，例如，Secure/Multipurpose Internet Mail Extensions (S/MIME)、SSL、EFS、IPSec 以及智慧卡登入。Windows Server 2003 支援多階層的 CA 架構，以及離線和線上作業的 CA 的跨驗證信任網路。

停用這服務會導致憑證需求無法被接受，CRL 和 delta CRL 也將不被發行。停止此服務太久將導致 CRL 過期，及確認已存在憑證的過程失敗。基於這些理由，在本手冊定義的企業用戶端環境中，這些服務的這設定值是設定成 Automatic (自動)。

電腦瀏覽器

表 10.5：設定值

服務名稱	成員伺服器預設值	企業用戶端
瀏覽	自動	停用

Computer Browser 服務會維護網路上最新的電腦清單，並提供此清單給要求它的程式。以 Windows 為基礎的電腦是使用 Computer Browser 這服務來檢視網路網域和資源。

指定作為瀏覽器的電腦，會維護包含所有網路上共用資源的瀏覽清單。較早版本的 Windows 應用程式，例如 My Network Places、NET VIEW 指令以及 Windows NT[®] Explorer 都需要這個瀏覽功能。舉例來說，在執行 Windows 95 的電腦上開啓 My Network Places 會顯示一個網域和電腦的清單，就是這電腦從指定作瀏覽器的電腦中複製瀏覽清單後所得到的。

電腦在一個瀏覽環境還可能會執行其他幾種不同角色。在某些情況下，例如，所指定作瀏覽器的電腦執行失敗或當機，瀏覽器—或潛在的瀏覽器—也許會改變成另一個不同的運作角色。

停用 Computer Browser 這服務會造成瀏覽器清單不能作更新或進行維護，而仰賴此服務的那些服務就無法啓動。不過，CA 伺服器並不需要這服務。因此，在本手冊所定義的企業用戶端系統環境中，此設定值是設定成停用。

其他登錄設定

其他登錄值項目，會為憑證服務伺服器的安全性範例檔案而建立，這些項目是在本手冊定義的企業用戶端環境的管理範例 (Administrative Template) .adm 檔案中沒有定義的。這些 .adm 檔案定義了有關 Windows Server 2003 的桌面、shell 及安全性設定的系統原則和限制。

這些額外的登錄設定在安全性範例中是自動更改的。如果移除了對應環境的原則，它的設定並不會自動被移除；必須用像 Regedt32.exe 這種登錄編輯工具手動地更改。

登錄設定在 Windows Server 2003 中，可以在「群組原則物件編輯器」中的底下這位置設定：

MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration

以下這表包括了含機碼 (key) 和子機碼 (subkey) 的登錄路徑，用以稽核任何對本手冊中所定義企業用戶端環境之憑證服務伺服器角色設定值的改變。

表 10.6：登錄稽核 SACL

UI 中的稽核路徑	企業用戶端
MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration (及其所有子機碼)	Failed; Everyone Full Control; <not inherited> Special
MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration (及其所有子機碼)	Success; Everyone; Special:Set Value, Create Subkey, Create Link, Delete, Change permissions, Take ownership; <not inherited> Special

其他安全性設定

以下設定可經由群組原則指定。但是，本手冊並未包含這些設定，因為每台伺服器所安裝的資料庫和記錄檔都可能不同。例如，您的憑證服務伺服器可能有 C:\、D:\ 及 E:\ 磁碟機。有關如何手動實作這些設定的細節大綱列於下面這一小節中。

檔案系統 ACL

沒有被存取控制清單 (access control lists，簡稱為 ACL) 保護的檔案會很容易被未經授權、但可以由本機或透過網路存取他們的使用者檢視、更改或刪除。ACL 主要是協助保護他們。而加密機制則提供了更好的保護，對於那些只有單一使用者需要存取的檔案是個不錯的方法。

下表包括了為本手冊所定義企業用戶端環境中、以 Windows Server 2003 為基礎、執行憑證服務伺服器的檔案系統的 ACL。在這環境中，憑證服務伺服器的憑證資料庫檔案夾是安裝在 D:\ 磁碟的 D:\CertSrv，資料庫記錄檔則儲存在預設資料夾 %SystemRoot%\system32\CertLog 中。記錄檔也可能由系統磁碟搬移到另一個實體是分開的鏡射磁碟，例如 E:\ 的 E:\CertLog 資料夾中。把資料庫和記錄檔放在不同磁碟中並非安全性的需求，不過我們建議把這些項目放在實體上分開的磁碟裝置，因為這樣能加強保護磁碟失敗及增進效能。憑證服務預設的安裝資料夾「%SystemRoot%\system32\CertLog」和「%SystemRoot%\system32\CertSrv」，其預設狀態是正確的 ACL。這些都顯示於下面這表中。

表 10.7：檔案系統

UI 中 ACL 路徑	企業用戶端
%SystemRoot%\system32\CertLog (傳播到所有子檔案夾)	Administrators (Full Control) SYSTEM (Full Control)
%SystemRoot%\system32\CertSrv (傳播到所有子檔案夾)	Administrators (Full Control) SYSTEM (Full Control) Users (Read and Execute, List Folder Contents, and Read)
D:\CertLog	Administrators (Full Control) SYSTEM (Full Control)
D:\CertSrv	Administrators (Full Control) SYSTEM (Full Control) Users (Read and Execute, List Folder Contents, and Read)

由於 CA 對安全性相當敏感的特質，上表中在憑證服務資料夾中的檔案稽核是設為啓用的。稽核項目設定如下：

表 10.8：憑證服務檔案和登錄稽核

檔案路徑或登錄路徑	稽核型態	稽核設定
%SystemRoot%\system32\CertLog	失敗	每個人 (完全控制)
%SystemRoot%\system32\CertSrv	成功	每個人(修改)
D:\CertSrv	成功	每個人(修改)
D:\CertLog	成功	每個人(修改)

這些設定的效用，是在稽核任何使用者對任何類型的檔案的失敗存取（讀或更改），以及稽核任何使用者成功的更改動作。

保護知名帳戶

Windows Server 2003 擁有許多內建使用者帳戶，是無法刪除但可重新命名的。Windows 2003 內兩個最有名的內建帳戶為 Guest 與 Administrator。

在預設狀態下，Guest 帳戶在成員伺服器 and 網域控制站上 are 停用的。此設定不建議變更。內建的 Administrator 帳戶應該重新命名，而描述也應改變，以防止駭客使用知名的帳戶危害遠端的伺服器。

許多惡意程式碼的變型都在初次嘗試中使用內建的管理員帳戶來危害伺服器。近年來，此組態變更的價值已逐漸減少，因為現在嘗試侵入伺服器的攻擊工具會指定內建 Administrator 帳戶的安全性識別項 (SID) 來決定其真正的名稱。SID 指的是可唯一識別網路上每個使用者、群組、電腦帳戶和登入工作階段的數值。您不可能變更此內建帳戶的 SID。將本機管理員帳戶重新命名為唯一的名稱，可讓您的作業群組監視嘗試攻擊此帳戶的事件。

請照以下步驟完成對網路上知名帳戶的保護：

1. 在每個網域和伺服器上，重新命名 Administrator 和 Guest 帳戶，並將其密碼變更為長而複雜的值。
2. 在伺服器上使用不同的名稱和密碼。若所有的網域和伺服器上都使用相同的帳戶名稱和密碼，可存取某台成員伺服器的駭客即可以相同的帳戶名稱和密碼來存取所有其他的伺服器。
3. 將帳戶描述變更為預設值以外的值，以防止他人輕易地識別出帳戶。
4. 將這些變更記錄在安全的位置。

注意：內建的 Administrator 帳戶可透過群組原則來重新命名。此設定值並未設定於本手冊所提供的任何安全性範本內，因為您應替您的環境選擇唯一的名稱。您可設定「Accounts : Rename administrator account 設定值」，以便將此手冊所定義三個環境中的管理員帳戶全都重新命名。此設定值是 GPO 的安全性選項設定的一部份。

保護服務帳戶

除非絕對必要，否則千萬不要將服務設定成在網域帳戶的安全性內容底下執行。若伺服器已受到實質的危害，他人即可透過傾印 Local Security Authority (本機的安全性授權單位，簡稱為LSA) 秘密，輕鬆取得網域帳戶的密碼。

摘要

本章解釋了補強本手冊所定義企業用戶端環境中、Windows Server 2003 的憑證服務伺服器之安全性設定。所討論的設定都是使用群組原則去設定與套用的。群組原則物件 (GPO) 是設計用來補足連結至網域控制站組織單位 (OU) 的「預設網域控制站原則」。「網域控制站基礎原則」(DCBP) 所包含的設定，將在任何給定的環境中，增強整個網域控制站的整體安全性。

詳細資訊

底下的資訊來源列出了在本產品發行之際，本手冊中詳細談到的 Windows Server 2003 和憑證服務伺服器角色密切相關的最新主題。

有一篇對公開金鑰基礎架構 (PKI) 的觀念和 Windows 2000 憑證服務的功能很好的簡介，請參閱 “An Introduction to the Windows 2000 Public-Key Infrastructure”，網址為 <http://www.microsoft.com/technet/prodtechnol/windows2000serv/evaluate/featfunc/pkiintro.asp>。

如需 Windows Server 2003 和 Windows XP 中 PKI 功能的詳細資訊，請參閱 “PKI Enhancements in Windows XP Professional and Windows Server 2003”，網址為 <http://www.microsoft.com/windowsxp/pro/techinfo/planning/pkiwinxp/default.asp>。

如需更多對 PKI 主要觀念背景的瞭解，請參閱 TechNet 上有關 “Public Key Infrastructure” 的資訊，網址為 http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/SE_PKI.asp。

11. 補強防禦主機

概觀

本章的重點在於補強您環境中的防禦主機。防禦主機是一台安全但可公開存取的電腦。防禦主機位於周邊網路的公用端 (亦稱為 DMZ、非軍事區和篩選子網路)。防禦主機可被防火牆或篩選路由器解除保護，導致它們完全暴露於攻擊底下。由於此暴露，您必須花更多的功夫來設計與設定防禦主機，來使它們受到危害的機會降至最低。

防禦主機一般用作為 Web 伺服器、Domain Name System (網域名稱系統，DNS) 伺服器、File Transfer Protocol (檔案傳輸通訊協定，FTP) 伺服器、Simple Mail Transport Protocol (簡單郵件傳輸通訊協定，SMTP) 伺服器和 Network News Transfer Protocol (網路新聞傳輸通訊協定，NNTP) 伺服器。在理想狀況下，防禦主機最好專門執行上述的某項功能，因為每台主機必須扮演的角色越多，忽略某個安全性漏洞的可能性就越大。您可以更輕鬆地在單一的防禦主機上保護單一服務。若企業組織付得起多台防禦主机的成本，便可大大受惠於這類網路架構。安全防禦主机的組態和一般的主機差異很大。所有沒必要的服務、通訊協定、程式和網路介面都會被停用或移除，之後每台防禦主機一般會被設成執行特定的角色。以此方式來補強防禦主機，將可限制可能的攻擊方法。

本章的下列章節將詳細地說明最能在任何環境中有效地保護防禦主机的各種安全性補強設定。

防禦主機本機原則

和本手冊先前所述其他伺服器角色的群組原則不同的是，群組原則並不能套用至防禦主機伺服器，因為它們都設成不屬於 Microsoft® Active Directory® 網域的獨立主機。由於其公開程度極高，本手冊所定義三個環境中的防禦主機只規定了一層指引。底下所述的安全性設定值乃以第三章「建成立員伺服器基礎」所定義高安全性環境的成員伺服器基礎原則 (Member Server Baseline Policy，簡寫為 MSBP) 為基礎。它們都包含於一個安全性範本內，此範本必須套用至每個防禦主机的防禦主機本機原則 (Bastion Host Local Policy，簡寫為 BHLPL) 中。

套用防禦主機本機原則

本手冊所包含的 High Security - Bastion Host.inf 檔可用來設定 BHLF。它將會啓用 SMTP 防禦主機正常運作所需的服務。套用 High Security - Bastion Host.inf 可大幅降低防禦主機的攻擊弱點，進而增強伺服器的安全性，但也會讓您無法從遠端管理防禦主機。BHLF 必須加以修改才能夠啓用任何進一步的功能，或增加防禦主機的管理性。

為了套用此安全性範本所包含的所有安全性設定，您必須使用 Security Configuration and Analysis 嵌入式管理單元，而非 Local Computer Policy 嵌入式管理單元。您並無法使用 Local Computer Policy 嵌入式管理單元來匯入安全性範本，因為系統服務的安全性設定值並無法使用此嵌入式管理單元來套用。

下列步驟詳述了使用 Security Configuration and Analysis 嵌入式管理單元來匯入與套用 BHLF 安全性範本的流程。

警告：微軟強烈地建議您先完整地備份防禦主機伺服器，再將 High Security - Bastion Host.inf 套用至它們之上。套用完 High Security - Bastion Host.inf 安全性範本之後，若想再將防禦主機還原成原本的組態，將會非常困難。請確認安全性範本已設成啓用您環境所需的防禦主機功能。

- 若要匯入安全性範本：
 1. 啓動 Security Configuration and Analysis 嵌入式管理單元。
 2. 以滑鼠右鍵按一下 Security Configuration and Analysis 範圍項目。
 3. 按一下 Open Database。
 4. 鍵入新的資料庫名稱，接著按一下 Open。
 5. 選取 High Security - Bastion Host.inf 安全性範本，接著按一下 Open。

這將會匯入所有的防禦主機設定值，之後您就可以檢視與套用它們。

- 若要套用安全性設定：
 1. 以滑鼠右鍵按一下 Security Configuration and Analysis 範圍項目。
 2. 選取 Configure Computer Now。
 3. 在 Configure Computer Now 對話方塊中鍵入想要檢視的記錄檔名稱，然後按一下 OK。

執行完這些步驟，就可將所有相關的安全性範本設定值套用到您環境中防禦主機的本機原則上。您必須重新啓動防禦主機，所有的設定才會生效。

下列的章節將描述以 BHLF 套用的安全性設定值。本章只記錄了與 MSBP 不同的設定值。

稽核原則設定

防禦主機的 BHP 稽核原則設定值就和 High Security - Member Server Baseline.inf 檔所指定的值完全相同。如需 MSBP 的詳細資訊，請參閱第三章「建成立員伺服器基礎」。MSBP 設定值可確保所有相關的安全性稽核資訊都記錄於所有的防禦主機伺服器上。

使用者權限設定

防禦主機的 BHLF 使用者權限設定乃以第三章「建成立員伺服器基礎」內的 High Security - Member Server Baseline.inf 檔所指定的值為基礎。BHLF 和 MSBP 之間的差異描述如下。

允許登入本機

表 11.1：設定值

成員伺服器預設值	設定值
Allow log on locally	管理員

Allow log on locally (允許登入本機) 使用者權限可讓使用者在電腦上啟動互動式工作階段。限制用來登入至防禦主機伺服器主控台的帳戶，將有助於防止他人擅自存取伺服器的檔案系統和系統服務。因為可登入至伺服器主控台的使用者可以運用該系統來危害其安全性。

Account Operators、Backup Operators、Print Operators 和 Power Users 群組在預設狀態下，都將擁有登入本機的權限。將此權限只授與 Administrators 群組，可防禦主機伺服器的管理存取限於極可靠的使用者，因而提供更大的安全性。

拒絕從網路存取本電腦

表 11.2：設定值

成員伺服器預設值	設定值
SUPPORT_388945a0	ANONONYMOUS LOGON; 內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶

注意：ANONONYMOUS LOGON、內建管理員、Support_388945a0、Guest 和所有非作業系統服務的帳戶都未包含於安全性範本內。這些帳戶和群組都擁有唯一的安全性識別項 (SID)。因此，它們必須以手動方式將其加到 BHLF 中。

Deny access to this computer from the network(拒絕從網路存取本電腦) 此使用者權限可決定哪些使用者無法存取網路上的電腦。此設定將會拒絕許多網路通訊協定，包括了以伺服器訊息區塊 (SMB) 為基礎的通訊協定、網路基本輸入/輸出系統 (NetBIOS)、Common Internet File System (CIFS)、Hypertext Transfer Protocol (HTTP) 和 Component Object Model Plus (COM+)。若此設定值和「Access this computer from the network(拒絕從網路存取本電腦)」同時控制使用者帳戶，此設定值會蓋過「Access this computer from the network(拒絕從網路存取本電腦)」設定值。若替其他群組設定此使用者權限，可能會造成使用者在您的環境中執行委派管理工作的能力受限。

在第三章「建成立員伺服器基礎」中，此手冊建議將 Guests 群組包含於指定了此權限的使用者和群組清單內，以提供最高等級的安全性。不過，用來匿名存取 IIS 的 IUSR 帳戶在預設狀態下為 Guests 群組的成員。基於這些理由，本手冊所定義的高安全性環境將防禦主機的「Access this computer from the network(拒絕從網路存取本電腦)」設定值設成包含了 ANONYMOUS LOGON; 內建管理員; Support_388945a0; Guest; 所有非作業系統服務的帳戶。

安全性選項

防禦主機的 BHLF 安全性選項設定就和第三章「建立成員伺服器基礎」的 High Security - Member Server Baseline.inf 檔所指定的值完全相同。BHLF 設定值可確保所有相關的安全性選項都一致地設定在所有的防禦主機伺服器上。

事件記錄檔設定

防禦主機的 BHLF 事件記錄檔設定就和第三章「建立成員伺服器基礎」的 High Security - Member Server Baseline.inf 檔所指定的值完全相同。BHLF 設定可確保所有相關的事件記錄檔設定都一致地設定在所有的防禦主機伺服器上。

系統服務

防禦主機伺服器原本就很容易遭受外界的攻擊。基於此理由，每台防禦主機的被攻擊弱點必須降至最少。為了妥善地補強防禦主機伺服器，作業系統不需用到的所有服務，以及非防禦主機角色正常運作所需的服務都應予以停用。本手冊所包含的 High Security - Bastion Host.inf 安全性範本會設定 BHLP，讓它啟用 SMTP 防禦主機伺服器正常運作所需的服務。BHLP 啓用了 Internet Information Services Manager 服務、HTTP SSL 服務和 SMTP 服務。不過，您還需要修改 BHLP 以啓用任何其他的功能。

大量的停用服務可能會產生許多被忽略的事件記錄檔警告。在某些狀況下，啓用這些服務的其中一部份反而可減少事件記錄檔的警告和錯誤訊息，並增加防禦主機的管理性。不過，這同時也是會增加每台防禦主機的被攻擊弱點。

底下章節將討論哪些服務應防禦主機伺服器上設成停用，以減少其被攻擊弱點，同時又維護其功能。只在 High Security - Member Server Baseline.inf 檔內尚未被停用的服務會包含在這些章節內。

自動更新

表 11.3：設定值

服務名稱	設定值
Wuau servicing	停用

Automatic Updates(自動更新) 服務可讓防禦主機下載與安裝重要的 Microsoft Windows® 更新資料。此服務會自動將最新的更新資料、驅動程式和增強功能提供給防禦主機。您不用再手動地搜尋重要的更新和資訊；作業系統會將它們直接提供給防禦主機。作業系統會知道您何時上線，並透過 Windows Update 服務，以您的 Internet 連線去搜尋適用的更新資料。根據您的組態設定，該服務可在下載、安裝之前通知您，或是自動替您安裝更新項目。

停止或停用 Automatic Updates 服務將會使得重要的更新無法自動下載至電腦。在此狀況下，您需要直接到 Windows Update 網站 <http://www.windowsupdate.microsoft.com> 中搜尋、下載與安裝任何適用的重要修復程式。

這項服務並不是讓防禦主機正常運作的必要項目。透過以本機原則來保護與設定此服務的起動模式，系統便可將存取權限只授與伺服器系統管理員，因此可防止未授權或惡意的使用者設定或操作該服務。再者，停用此服務可有效地減少防禦主機伺服器的被攻擊弱點。基於這些理由，Automatic Updates 設定值在 BHLP 中將設成停用。

Background Intelligent Transfer Service

表 11.4：設定值

服務名稱	設定值
BITS	停用

Background Intelligent Transfer Service (BITS) 是一個背景檔傳輸機制和佇列管理員。BITS 可以非同步地在用戶端和 HTTP 伺服器之間傳送檔案。BITS 可接受請求而以閒置的網路頻寬來傳送檔案，因此其他的網路相關活動，例如瀏覽，並不會受到影響。

停止此服務將導致 Automatic Update 等功能無法自動下載程式和其他資訊，直到服務再次執行為止。這意味著若此服務已透過群組原則來設定，電腦將不會從 Software Update Services (SUS) 收到自動的更新。停用此服務將導致倚賴它的任何服務無法傳送檔案，除非某個失敗-安全機制已就緒，可直接透過其他方法 (例如 Internet Explorer) 來傳送檔案。

此服務並非讓防禦主機正常運作的必要項目。透過以本機原則來保護與設定此服務的起動模式，系統可將存取權限僅授與伺服器系統管理員，因此可防止未授權或惡意的使用者設定或操作該服務。再者，停用此服務可有效地減少防禦主機伺服器的被攻擊弱點。基於這些理由，此服務在 BHLF 中將設成停用。

電腦瀏覽器

表 11.5：設定值

服務名稱	設定值
Browser	停用

Computer Browser 服務將維護您網路上的最新電腦清單，並提供該清單給要求它的程式。Computer Browser 服務將由需要檢視網路網域和資源的 Windows 型態電腦所使用。指定成瀏覽器的電腦會維護瀏覽清單，這裡面包含了用於網路上的所有共用資源。Windows 應用程式的較早版本，例如 My Network Places、NET VIEW 指令 and Microsoft Windows NT® Explorer 都需要瀏覽功能。例如，在執行 Windows 95 的電腦上開啓 My Network Places 將會顯示一個網域和電腦清單，此清單是由該電腦向被指定為瀏覽器的電腦所取得的瀏覽器清單複本。

停用 Computer Browser 服務將導致瀏覽器清單無法更新或維護。停用此服務將導致確實倚賴它的任何服務失敗。

此服務並非讓防禦主機正常運作的必要項目。透過以本機原則來保護與設定此服務的起動模式，系統可將存取權限只授與伺服器系統管理員，因此可防止未授權或惡意的使用者設定或操作該服務。再者，停用此服務可有效地減少防禦主機伺服器的被攻擊弱點。基於這些理由，Computer Browser 設定值在 BHLF 中將設成停用。

DHCP 用戶端

表 11.6：設定值

服務名稱	設定值
Dhcp	停用

DHCP Client 服務將透過註冊和更新您電腦的 Internet Protocol (IP) 位址與 DNS 名稱來管理網路組態。當用戶端 (例如漫遊使用者) 在網路內閒逛時，此服務可讓您不需手動地變更 IP 設定。不管用戶端重新連接到哪個子網路，該用戶端都會自動被賦予一個新的 IP 位址 – 只要 Dynamic Host Configuration Protocol (DHCP) 伺服器可從這每一個子網路中存取。您不需要手動地替 DNS 或 Windows Internet Name Service (WINS) 設定設定值。只要 DHCP 伺服器被設成發出這類資訊，DHCP 伺服器就可將這些服務設定值強制應用到用戶端上。若要在用戶端上啟用此選項，只要選取 Obtain DNS Server Address Automatically 選項按鈕即可。啟用此選項並不會導致重複的 IP 位址衝突。

停止 DHCP Client 服務將使您的電腦無法收到動態的 IP 位址，同時自動化的 Dynamic DNS 更新也不會在 DNS 伺服器上註冊。停用此服務將導致確實倚賴它的任何服務失敗。

此服務並非讓防禦主機正常運作的必要項目。透過以本機原則來保護與設定此服務的起動模式，系統可將存取權限只授與伺服器系統管理員，因此可防止未授權或惡意的使用者設定或操作該服務。再者，停用此服務可有效地減少防禦主機伺服器的被攻擊弱點。基於這些理由，DHCP Client 設定值在 BHLP 中將設成停用。

Network Location Awareness (NLA)

表 11.7：設定值

服務名稱	設定值
Lanmanserver	停用

Network Location Awareness (NLA) 服務會收集和儲存網路組態資訊，例如 IP 位址和網域名稱變更，以及位置變更資訊，並在此資訊變更時通知應用程式。

此服務並非讓防禦主機正常運作的必要項目。透過以本機原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器系統管理員，因此可防止未授權或惡意的使用者設定或操作該服務。再者，停用此服務可有效地減少防禦主機伺服器的被攻擊弱點。基於這些理由，Network Location Awareness (NLA) 設定值在 BHLP 中將設成停用。

NTLM 安全性支援提供者

表 11.8：設定值

服務名稱	設定值
NtLmSsp	停用

NTLM Security Support Provider 服務提供安全性給使用傳輸、而非具名管道 (Named Pipe) 的遠端程序呼叫 (RPC) 程式，並讓使用者使用 NTLM 驗證通訊協定來登入至網路。NTLM 通訊協定會驗證不使用 Kerberos 5 版驗證的用戶端。

停止或停用 NTLM Security Support Provider 服務將令您無法使用 NTLM 驗證通訊協定來登入至用戶端，或存取網路資源。Microsoft Operations Manager (MOM) 和 Telnet 都倚賴此服務。

此服務並非讓防禦主機正常運作的必要項目。透過以本機原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器系統管理員，因此可防止未授權或惡意的使用者設定或操作該服務。再者，停用此服務可有效地減少防禦主機伺服器的被攻擊弱點。基於這些理由，NTLM Security Support Provider 設定值在 BHLP 中應設成停用。

執行效能記錄與警示

表 11.9：設定值

服務名稱	設定值
SysmonLog	停用

mance Logs and Alerts 服務會根據預先設定的排程參數，向本機或遠端電腦收集效能資料，接著將資料寫至記錄檔或觸發一個警示。Performance Logs and Alerts 服務會根據具名記錄檔收集設定內所包含的資訊，啟動和停止收集每個具名的效能資料。此服務只會在至少排程了一個收集時進行執行的動作。

停止或停用 Performance Logs and Alerts 服務將導致效能資訊無法收集、目前執行的資料收集將會中止、未來的排程收集不會發生。

此服務並非讓防禦主機正常運作的必要項目。透過以本機原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器系統管理員，因此可防止未授權或惡意的使用者設定或操作該服務。再者，停用此服務可有效地減少防禦主機伺服器的被攻擊弱點。基於這些理由，Performance Logs and Alerts 設定值在 BHLP 中應設成停用。

遠端系統管理服務

表 11.10：設定值

服務名稱	設定值
SrvcSurg	停用

Remote Administration Service 將在伺服器重新啟動時，執行下列的遠端管理工作：

- 增加伺服器的重新啟動帳戶。
- 產生自我簽章的認證。
- 若日期和時間未設定於伺服器上，將會引發一個警示。
- 若警示電子郵件 (Alert E-mail) 功能尚未設定，將會引發一個警示。

停止 Remote Administration Service 可能導致 Remote Server Administration Tools 的一些功能無法適當地運作，例如遠端管理的 Web 介面。停用此服務將導致確實倚賴它的任何服務失敗。

此服務並非讓防禦主機正常運作的必要項目。透過以本機原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器系統管理員，因此可防止未授權或惡意的使用者設定或操作該服務。再者，停用此服務可有效地減少防禦主機伺服器的被攻擊弱點。基於這些理由，Remote Administration Service 設定值在 BHLPL 中應設成停用。

遠端註冊服務

表 11.11：設定值

服務名稱	設定值
RemoteRegistry	停用

在遠端使用者擁有必要的權限下，Remote Registry Service 可讓遠端使用者修改網域控制站上的登錄設定值。在預設狀態下，只有 Administrators 和 Backup Operators 群組中的使用者可從遠端存取登錄資料。此服務對於 Microsoft Baseline Security Analyzer (MBSA) 公用程式是必要的。MBSA 工具可讓您確認哪些修補程式已安裝在您組織中的每台伺服器上。

若停止 Remote Registry Service，您就只能修改本機電腦上的登錄。停用此服務將導致確實倚賴它的任何服務執行失敗，但是不會影響您本機電腦上的登錄作業。其他的電腦或裝置也不會再連接至您本機電腦的登錄。

此服務並非讓防禦主機正常運作的必要項目。透過以本機原則來保護與設定服務的起動模式，系統可將存取權只授與伺服器系統管理員，因此可防止未授權或惡意的使用者設定或操作該服務。再者，停用此服務可有效地減少防禦主機伺服器的被攻擊弱點。基於這些理由，Remote Registry Service 設定值在 BHLPL 中應設成停用。

伺服器

表 11.12：設定值

服務名稱	設定值
Lanmanserver	停用

Server 服務在網路上提供了 RPC 支援、檔案、列印和具名管道共用。此服務可提供本機資源共用，例如磁碟和印表機，以便讓網路上的其他使用者存取它們。它也可在執行於其他電腦和您用於RPC的電腦上的應用程式之間提供具名管道的通訊。具名管道通訊指的是一塊保留的記憶體，可讓某個處理序的輸出作為另一個處理序的輸入。接受輸入的處理序並不需要位於電腦本機。

若停止 Server 服務，您就無法將電腦上的檔案和印表機分享給網路上的其他電腦使用，它也無法滿足 RPC 要求。停用此服務將導致倚賴它執行的任何服務執行失敗。

此服務並非讓防禦主機正常運作的必要項目。透過以本機原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器系統管理員，因此可防止未授權或惡意的使用者設定或操作該服務。再者，停用此服務可有效地減少防禦主機伺服器的被攻擊弱點。基於這些理由，Server 設定值在 BHLF 中應設成停用。

TCP/IP NetBIOS Helper Service

表 11.13：設定值

服務名稱	設定值
LMHosts	停用

TCP/IP NetBIOS Helper Service 可在 TCP/IP (NetBT) 服務上支援網路基本輸入/輸出系統 (NetBIOS)，並替您網路上的用戶端提供 NetBIOS 名稱解析；因此可讓使用者共用檔案、列印與登入至網路。Transmission Control Protocol/Internet Protocol (TCP/IP) NetBIOS Helper 服務可透過執行 DNS 名稱解析來支援 NetBT 服務。

停止 TCP/IP NetBIOS Helper Service 將令 NetBT、Redirector (RDR)、Server (SRV)、Netlogon 和 Messenger 服務用戶端無法共用檔案、印表機，而使用者也無法登入至電腦。例如，以網域為基礎的群組原則將無法再作用。停用此服務將導致倚賴它執行的任何服務執行失敗。

此服務並非讓防禦主機正常運作的必要項目。透過以本機原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器系統管理員，因此可防止未授權或惡意的使用者設定或操作該服務。再者，停用此服務可有效地減少防禦主機伺服器的被攻擊弱點。基於這些理由，TCP/IP NetBIOS Helper Service 設定值在 BHLF 中應設成停用。

終端機服務

表 11.14：設定值

服務名稱	設定值
TermService	停用

Terminal Services 提供了多重工作階段的环境，可讓用戶端裝置存取執行於伺服器上的虛擬 Windows desktop 工作階段和 Windows 型態的程式。Terminal Services 可讓使用者從遠端管理伺服器。

停止或停用 Terminal Services 將令您無法從遠端管理電腦，進而很難管理及更新電腦。

此服務並非讓防禦主機正常運作的必要項目。透過以本機原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器系統管理員，因此可防止未授權或惡意的使用者設定或操作該服務。再者，停用此服務可有效地減少防禦主機伺服器的被攻擊弱點。基於這些理由，Terminal Services 設定值在 BHLP 中應設成停用。

Windows Installer

表 11.15：設定值

服務名稱	設定值
MSIServer	停用

Windows Installer 服務將在安裝過程中套用一組集中定義的設定規則，藉此管理應用程式的安裝與移除。這些設定規則會定義所安裝應用程式的安裝與組態。此外，此服務亦可用來修改、修復或移除現有的應用程式。此服務的技術包括了 Windows 作業系統的 Windows Installer 服務，以及用來包含應用程式設定與安裝相關資訊的 (.msi) 封裝檔案格式。

Windows Installer 並不只是安裝程式；它也是可擴充的軟體管理系統。此服務可管理安裝、新增和刪除軟體元件、監視檔案回復能力、使用復原功能維護基本的檔案災害復原。此外，Windows Installer 支援從多重來源安裝與執行軟體，並可由想要安裝自訂應用程式的開發人員自行設定。

將 Windows Installer 設成手動，會使得使用安裝程式的應用程式啟動此服務。

停止此服務將令您無法再安裝、移除、修復和修改倚賴它的應用程式。此外，執行時會用到此服務的一些應用程式可能無法執行。停用此服務將導致倚賴它執行的任何服務執行失敗。

此服務並非讓防禦主機正常運作的必要項目。透過以本機原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器系統管理員，因此可防止未授權或惡意的使用者設定或操作該服務。再者，停用此服務可有效地減少防禦主機伺服器的被攻擊弱點。基於這些理由，Windows Installer 設定值在 BHLP 中應設成停用。

Windows Management Instrumentation Driver Extensions

表 11.16：設定值

服務名稱	設定值
Lanmanserver	停用

Windows Management Instrumentation Driver Extensions 服務會監視已設成發行 WMI 或事件追蹤資訊的所有驅動程式和事件追蹤提供者。

此服務並非讓防禦主機正常運作的必要項目。透過以本機原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器系統管理員，因此可防止未授權或惡意的使用者設定或操作該服務。再者，停用此服務可有效地減少防禦主機伺服器的被攻擊弱點。基於這些理由，Windows Management Instrumentation Driver Extensions 設定值在 BHLP 中應設成停用。

WMI Performance Adapter

表 11.17：設定值

服務名稱	設定值
Lanmanserver	停用

WMI Performance Adapter 服務提供了來自 WMI HiPerf 提供者的效能程式庫資訊。今日需要提供效能計數器的應用程式和服務，可採用兩種方式來達成；透過編寫 WMI High Performance 提供者或編寫效能程式庫。

WMI Performance Adapter 服務會將 WMI High Performance 提供者所提供的效能計數器轉換成可透過 Reverse Adapter Performance Library 來供 Performance Data Helper (PDH) 消耗的計數器。透過此方式，PDH 用戶端 (例如 Sysmon) 可以消耗電腦上的任何 WMI High Performance 提供者所提供的效能計數器。若 WMI Performance Adapter 服務停止了，WMI 效能計數器便無法使用。停用此服務將導致倚賴它執行的任何服務執行失敗。

此服務並非讓防禦主機正常運作的必要項目。透過以本機原則來保護與設定服務的起動模式，系統可將存取權僅授與伺服器系統管理員，因此可防止未授權或惡意的使用者設定或操作該服務。再者，停用此服務可有效地減少防禦主機伺服器的被攻擊弱點。基於這些理由，WMI Performance Adapter 設定值在 BHLP 中應設成停用。

其他安全性設定

透過 MSBP 套用的安全性設定替防禦主機伺服器提供了許多增強的安全性。但還有一些額外的事項需要考慮。這些步驟並無法透過群組原則來完成，而應以手動方式在所有的防禦主機伺服器上執行。

手動地將唯一的安全性群組加至使用者權限設定內

大多數經由 MSBP 套用的使用者權限設定 (User Rights Assignments) 都有適當的安全性群組指定於本手冊所附的安全性範本內。不過，仍有一些帳戶和安全性群組無法包含於範本之中，因為其安全性識別項 (SID) 僅適用於個別的 Windows 2003 網域。可以手動設定的使用者權限設定如下所列。

警告：下表包含了內建 Administrator 帳戶的值。請勿將此帳戶和內建的 Administrators 安全性群組搞混了。若 Administrators 安全性群組已加至底下的任一個拒絕存取使用者權限中，您需要登入於本機來訂正此錯誤。此外，內建的 Administrators 帳戶可能已根據第三章「建立成員伺服器基礎」所述的一些建議重新命名。在加入 Administrator 帳戶時，請記得指定重新命名的帳戶。

表 11.18：手動加入使用者權限設定

成員伺服器預設值	舊版用戶端	企業用戶端	高安全性
拒絕從網路存取此電腦	內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶	內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶	內建管理員; Support_388945a0; Guest; 所有非作業系統服務的 帳戶

重要：所有非作業系統服務的帳戶包括了企業內特定應用程式所使用的服務帳戶。這並未包含 LOCAL SYSTEM、LOCAL SERVICE 或 NETWORK SERVICE 帳戶，它們都是作業系統使用的內建帳戶。

移除沒必要的網路通訊協定和繫結

可直接在 Internet 上存取的伺服器，特別是防禦主機伺服器，應該停用所有沒必要的通訊協定，以抵銷使用者列舉的威脅。使用者列舉指的是收集可運用機會的某類資訊，攻擊者可透過它，嘗試取得系統的相關資訊，以策劃進一步的攻擊。

伺服器訊息區塊 (Server Message Block，簡寫為 SMB) 通訊協定可使用“null”工作階段，傳回電腦的相關豐富資訊給使用者，甚至是未經驗證的使用者。可取得的資訊包括了共用區、使用者資訊 (包括群組和使用者權限)、登錄機碼等等。

停用 TCP/IP 上的 SMB 和 NetBIOS 可大大減少伺服器的被攻擊弱點，藉此保護防禦主機。雖然運作於此組態下的伺服器較難管理，並且無法存取共用於網路上的資料夾，但這些措施可有效地保護伺服器，不

讓它輕易地受到危害。因此，本手冊建議您替可從 Internet 存取的防禦主機伺服器上的網路連線，停用 TCP/IP 上的 SMB 和 NetBIOS。

- 若要停用 SMB：

1. 在 Control Panel 上，連按兩下 Network Connections。
2. 以滑鼠右鍵按一下連至 Internet 的連線，接著按一下 Properties。
3. 在 Properties 對話方塊中選取 Client for Microsoft Networks，接著按一下 Uninstall。
4. 執行解除安裝的步驟。
5. 選取 File and Printer Sharing for Microsoft Networks，接著按一下 Uninstall。
6. 執行解除安裝的步驟。

- 若要停用 TCP/IP 上的 NetBIOS：

1. 在 Control Panel 上連按兩下 System，按一下 Hardware 索引標籤，接著按 Device Manager 按鈕。
2. 在 View 功能表上按一下 Show hidden devices。
3. 展開 Non-Plug and Play Drivers。
4. 以滑鼠右鍵按一下 NetBIOS over Tcpip，接著按一下 Disable。

此程序將停用 TCP/445 和 UDP 445 上的 SMB 直接主機接聽項。

注意：此程序將停用 nbt.sys 驅動程式。Advanced TCP/IP Settings 對話方塊的 WINS 索引標籤包含了 Disable NetBIOS over TCP/IP 選項。選取此選項只會停用 NetBIOS Session Service (它會聆聽 TCP 連接埠 139)。它並不會完全停用 SMB。若要完全停用，請使用上述步驟。

保護知名帳戶

Microsoft Windows Server 2003 擁有許多無法刪除、但可重新命名的內建使用者帳戶。Windows 2003 內兩個最有名的內建帳戶為 Guest 與 Administrator。

在預設狀態下，Guest 帳戶將停用於伺服器上，並且不應變更。內建的 Administrator 帳戶應該重新命名，而描述也應改變，以防止攻擊者使用知名的帳戶危害遠端的伺服器。

許多惡意程式碼的變型都在初次嘗試中使用內建的管理員帳戶來危害伺服器。近年來，此組態變更的價值已逐漸減少，因為現在嘗試侵入伺服器的攻擊工具會指定內建 Administrator 帳戶的安全性識別項 (SID) 來決定其真正的名稱。SID 指的是可唯一識別網路上每個使用者、群組、電腦帳戶和登入工作階段的數值。您不可能變更此內建帳戶的 SID。若您將本機管理員帳戶重新命名為唯一的名稱，可讓您的作業群組監視嘗試攻擊此帳戶的事件。

• 要保護防禦主機伺服器上的知名帳戶：

1. 在每台伺服器上，重新命名 Administrator 和 Guest 帳戶，然後將其密碼變更為長而複雜的值。
2. 在伺服器上使用不同的名稱和密碼。若所有的伺服器上都使用相同的帳戶名稱和密碼，可存取某台伺服器的攻擊者即可以相同的帳戶名稱和密碼來存取所有其他的伺服器。
3. 將帳戶描述變更為預設值以外的值，以防止他人輕易地識別出帳戶。
4. 將這些變更記錄在安全的位置。

錯誤報告

表 11.19：設定值

預設值	舊版用戶端	企業用戶端	高安全性
Report Errors	停用	停用	停用

Error Reporting 服務可協助微軟追蹤和解決錯誤。您可設定此服務來替作業系統錯誤、Windows 元件錯誤或程式錯誤產生報告。啟用 Report Errors 服務將會透過 Internet 將這類錯誤報告給微軟，或報告給內部的公司檔案共用區。

此設定只能用於 Microsoft Windows® XP Professional 和 Windows Server 2003。在 Group Policy Object Editor 中設定此設定值的路徑為：

Computer Configuration\Administrative Templates\System>Error Reporting

錯誤報告可能包含敏感、甚至機密的公司資料。微軟錯誤報告的隱私權原則可確保微軟不至於不當地使用這類資料，不過由於資料是以 cleartext Hypertext Transfer Protocol (HTTP) 來傳送，它可能會在 Internet 上遭到攔截，並被協力廠商所檢視。基於這些理由，在本手冊所定義的三個安全性環境中，本手冊都建議您在 BHLP 中將 Error Reporting 設定值設成停用。

以 IPSec 篩選器封鎖連接埠

Internet Protocol Security (IPSec) 篩選器可提供有效的方法來增強伺服器所需的安全性等級。此手冊替手冊內所定義的高安全性環境建議此選擇性指引，以進一步地減少伺服器的被攻擊弱點。

如需使用 IPSec 篩選器的詳細資訊，請參閱下列隨附手冊的第 11 章「Additional Member Server Hardening Procedures」：《Threats and Countermeasures:

Security Settings in Windows Server 2003 and Windows XP》。

下表列出了所有可建立於本手冊所定義高安全性環境之 SMTP 防禦主機上的 IPSec 篩選器。

表 11.20：SMTP 防禦主機 IPSec 網路傳輸對應

服務	通訊協定	來源連接埠	目標連接埠	來源位址	目標位址	動作	鏡像
SMTP Service	TCP	任意	25	任意	ME	允許	是
DNS Client	TCP	任意	53	ME	DNS Server	允許	是
DNS Client	UDP	任意	53	ME	DNS Server	允許	是
所有傳入的 傳輸資料	任意	任意	任意	任意	ME	封鎖	是

上表所列的所有規則都應在實作時加以鏡像。這可確保傳入伺服器內的任何網路傳輸資料亦可回到原本的伺服器中。

上表代表了應開啓哪些基底連接埠，以便讓伺服器執行其特定角色的功能。若伺服器擁有靜態的 IP 位址，這些連接埠就已足夠。

警告：這些 IPSec 篩選器的限制相當多，並將大大降低這些伺服器的管理性。您將需要開啓額外的連接埠，方能啓用監視、修補程式管理和軟體更新功能。

實作 IPSec 原則應該不會嚴重地影響伺服器的效能。不過，您仍應在實作這些篩選器之前進行測試，以確保伺服器的必要功能和效能都可維持。您可能也需要加入額外的規則來支援其他應用程式。

本手冊包含了一個 .cmd 檔，簡化了建立適用於防禦主機的 IPSec 篩選器的工作。PacketFilters-SMTPBastionHost.cmd 檔使用 NETSH 命令來建立適當的篩選器。

此指令碼並不會建立永續性篩選器。因此，伺服器需等到 IPSec Policy Agent 啓動時才會受到保護。如需建立永續性篩選器或建立更進階 IPSec 篩選器指令碼的詳細資訊，請參閱下列所附手冊的第 11 章「Additional Member Server Hardening Procedures」：《Threats and Countermeasures：Security Settings in Windows Server 2003 and Windows XP》。最後，此指令碼已設定成不指定它建立的 IPSec 原則。IP Security Policy Management 嵌入式管理單元可用來檢查建立的 IPSec 篩選器，並指定 IPSec 原則，以便讓它生效。

摘要

防禦主機伺服器高度地暴露於外界的攻擊下。因此您必須儘可能地保護它們，以提供最大的可用性，並儘量減少防禦主機伺服器受到危害的影響。要擁有最安全的防禦主機伺服器，您必須只限制最可靠的帳戶具備存取權限，並只啓用須完整執行其功能所需的最少服務。

本章說明了用來保護防禦主機伺服器的預定伺服器補強設定和程序。這些設定中有許多可透過本機群組原則來套用。本章也提供了設定與套用手工設定的步驟。

此外，此處也提供建立與套用 IPsec 篩選器的細節，以控制可與防禦主機伺服器進行通訊的網路傳輸類型。您也可根據防禦主機伺服器在您環境中扮演的自訂角色，修改這些篩選器，以封鎖特定的網路傳輸類型。

詳細資訊

底下的資訊來源列出了在本產品發行之際，與執行 Windows Server 2003 的電腦所在環境中的防禦主機伺服器密切相關的最新主題。

如需防禦主機的詳細資訊，請參閱 Kevin Steves 所著的“Building a Bastion Host Using HP-UX 11”，網址為：
<http://people.hp.se/stevesk/bastion11.html>

如需建立私人網路的詳細資訊，請參閱 Elizabeth D. Zwicky、Simon Cooper 和 Brent D. Chapman 聯合著作的“Firewalls and Virtual Private Networks”，網址為：

http://www.wiley.com/legacy/compbooks/press/0471348201_09.pdf。

如需防火牆和安全性的進一步資訊，請參閱 Chuck Semeria 所著的“Internet Firewalls and Security - A Technology Overview”，網址為：

http://www.linuxsecurity.com/resource_files/firewalls/nsc/500619.html#Bastion%20Host。

如需深度防禦模型的相關資訊，請參閱“U.S. Military with Rod Powers”，網址為：

<http://usmilitary.about.com/careers/usmilitary/library/glossary/d/bldef01834.htm>。

如需防禦侵入者的相關資訊，請參閱 Jay Beale 所著的“Intruder Detection Checklist”，網址為：

http://www.cert.org/tech_tips/intruder_detection_checklist.html。

如需補強防禦主機的相關資訊，請參閱 SANS Info Sec Reading Room 的“Hardening Bastion Hosts”文章，網址為：http://www.sans.org/rr/securitybasics/hard_bastion.php。

如需防禦主機的進一步資訊，請參閱“How Bastion Hosts Work”，網址為：

<http://thor.info.uaic.ro/~busaco/teach/docs/intranets/ch16.htm>。

如需關閉 Windows Server 2003 內 Internet Connection Firewall 的相關資訊，請參閱知識庫文件“How To: Turn On the Internet Connection Firewall Feature in Windows Server 2003”，網址為：

<http://support.microsoft.com/default.aspx?scid=317530>。

如需安全性組態和分析工具的疑難排解相關資訊，請參閱知識庫文件，“Problems After You Import Multiple Templates Into the Security Configuration and Analysis Tool”，網址為：

<http://support.microsoft.com/default.aspx?scid=279125>。

如需網站安全性的相關資訊，請參閱“Site Security Handbook”，網址為：

<http://www.theinternetbook.net/rfc/rfc2196.html>。

12. 結論

恭喜你！讀完此手冊之後，想必您已更清楚地瞭解如何評估可能影響您組織中執行 Microsoft® Windows Server™ 2003 之電腦的安全性風險。相信您已知道如何將安全性儘可能地規劃與設計到您的基礎架構內。此手冊包含了適用於任何組織的指引。

手冊包含的題材乃由常在各種公司設定中實作 Windows Server 2003、Windows XP 和 Windows 2000 解決方案的實地顧問和系統工程師所提供，以期提供您目前執行此複雜工作的最佳實施方針。

不管您組織的環境為何，都應審慎地考量安全性。不過，還是有許多企業組織並不是很重視安全性，誤以為它是限制企業靈活度和彈性的項目。當精心設計的安全性成為核心的企業需求，並且每個資訊技術 (IT) 專案一開始就會針對它規劃帳戶時，妥善實作的安全性策略將有助於改善您電腦系統的可用性和效能。另一方面，若到後來才將安全性加至專案內，經常會對使用性、穩定性和管理彈性產生負面的影響 – 這些是為何每個組織都應將安全性視為最高優先的理由。

此手冊說明了在三個不同環境中如何有效地降低電腦執行 Windows Server 2003 的安全性風險。它提供了方法來規劃與設計安全性到您組織的網路基礎架構內，並詳細地指示您如何修正執行 Windows Server 2003 的電腦上常見的特定漏洞。

這些選擇背後的原因都根據利弊得失來加以解釋，它們通常用來決定是否替本手冊詳述的三個環境實作這每一個對策。此處也詳細地說明了特定對策如何影響電腦的功能、管理性、效能和可靠性，以便讓您在資訊充足的狀況下，決定將哪些對策實作於您自己的環境中。

最後，您務必了解保護您網路中伺服器的工作是一個無法停止的過程，絕非短期專案，組織必須將此過程納入企業的預算和排程之中。實作本章所探討的所有對策，將可改善大多數組織操作 Windows Server 2003 時的安全性。

不過，當下個嚴重的漏洞出現時，這些環境可能又會變得易受攻擊。基於這些原因，您務必監視各式資源，讓它們在您環境之作業系統、應用程式和裝置方面的安全性議題上，隨時保持最新狀態。

製作此手冊的每個團隊成員都竭誠地希望手冊所涵蓋的題材既有用、又廣博、並且易於瞭解。

詳細資訊

底下的資訊來源列出了在本產品發行之際，與 Windows Server 2003 密切相關的最新主題。

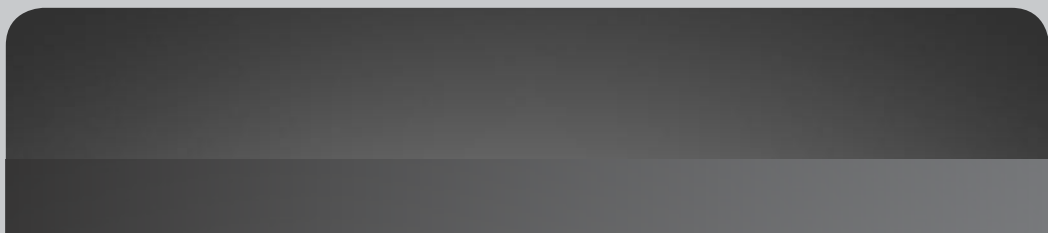
如需 Microsoft 公司安全性的詳細資訊，請參閱：<http://www.microsoft.com/security>。

如需 MOF 如何協助您企業的詳細資訊，請參閱：<http://www.microsoft.com/business/services/mcsmof.asp>。

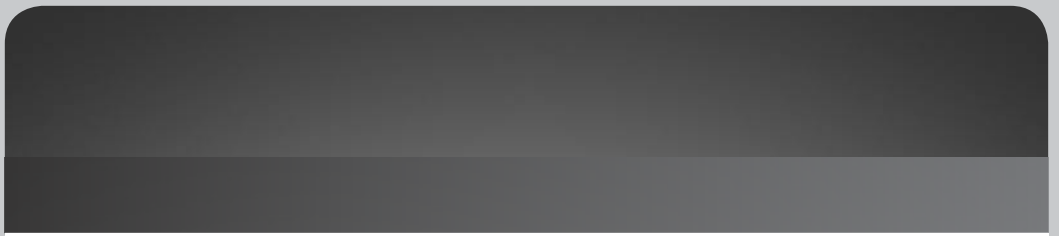
如需 Microsoft 策略科技保護計畫 (Microsoft Strategic Technology Protection Program) 的相關資訊，請參閱：
<http://microsoft.com/security/mstpp.asp>。

如需 Microsoft 安全性通知服務 (Microsoft Security Notification Service) 的相關資訊，請參閱：
<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp>。

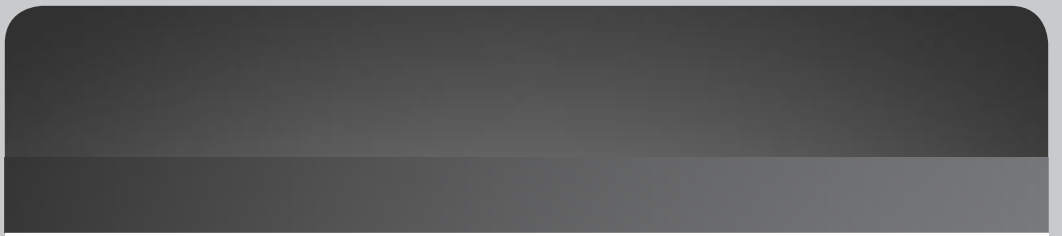
This image shows a single sheet of white paper with horizontal blue ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

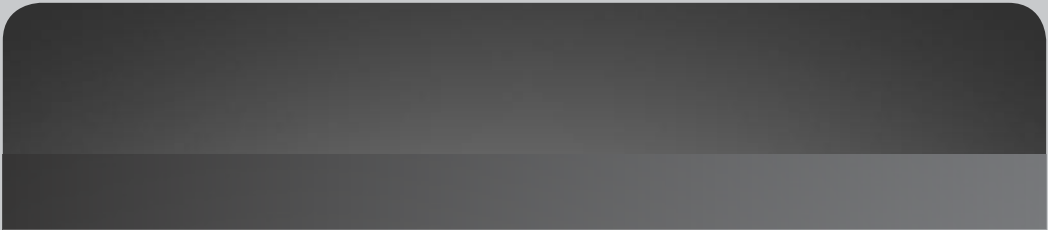
This image shows a single sheet of white paper with horizontal blue ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

This image shows a single sheet of white paper with horizontal blue ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.



Handwriting practice lines consisting of 18 horizontal lines. Each line is preceded by a small vertical tick mark on the left side, serving as a guide for letter height and placement.

This image shows a single sheet of white paper with horizontal blue ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



www.microsoft.com/taiwan/windowsserver2003

本文件的資訊，包括 URL 及其它網站參考資料，皆可能在未告知下變更。除非另有通知，本文件中所舉例之公司、機構、產品、網域名稱、電子郵件信箱、標誌、人物、地點及事件皆為虛構，並且未企圖影射任何實際公司、機構、產品、網域名稱、電子郵件信箱、標誌、人物、地點及事件等，也不應被聯想。遵守所有適用的著作權法是使用者的責任。在不限制著作權法所保障的權利下，若無微軟公司的書面許可，本文件的任何部分都不可重複生產、儲存或放入可存取的系統中，或以任何形式、方式 (不管是電子、機械、影印、錄音等方式) 或基於任何目的來傳輸。

微軟在本文件中可能擁有專利、專利應用程式、商標、著作權或其他智慧財產權所保護的題材。除非您取得微軟的任何書面授權合約外，本文件並未提供您這些專利、商標、著作權或其他智慧財產權的任何授權。

© 2003 Microsoft Corporation 版權所有。

Microsoft 和 Visual Basic 均為微軟公司在美國和 (或) 其他國家的註冊商標或商標。

此處所提及的真實公司與產品名稱皆為其各自所屬擁有者的商標。